Verständnis des Firewall-Designs mit zonenbasierten Richtlinien

Inhalt

Einleitung

In diesem Dokument wird das Konfigurationsmodell für die zonenbasierte Firewall (ZFW) der Cisco IOS® Firewall beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieses neue Konfigurationsmodell bietet intuitive Richtlinien für Router mit mehreren Schnittstellen, eine höhere Granularität der Anwendung von Firewall-Richtlinien und eine standardmäßige Deny-All-Richtlinie, die den Datenverkehr zwischen Firewall-Sicherheitszonen

untersagt, bis eine explizite Richtlinie angewendet wird, um den gewünschten Datenverkehr zuzulassen.

Nahezu alle klassischen Funktionen der Cisco IOS Firewall, die vor Version 12.4(6)T der Cisco IOS Software implementiert wurden, werden von der neuen zonenbasierten Richtlinieninspektionsschnittstelle unterstützt:

- Stateful Packet Inspection
- VRF-kompatible Cisco IOS Firewall
- URL-Filterung
- DoS-Eindämmung (Denial of Service)

Mit der Cisco IOS Software-Version 12.4(9)T profitieren Sie von ZFW-Unterstützung für Session-/Verbindungs- und Durchsatzbeschränkungen pro Klasse sowie von Anwendungsinspektion und -kontrolle:

- HTTP
- Post Office Protocol (POP3), Internet Mail Access Protocol (IMAP), Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
- Sun Remote Procedure Call (RPC)
- Instant Messaging (IM)-Anwendungen:Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- Peer-to-Peer (P2P)-Dateifreigabe:BittorrentKaZaAGnutellaeDonkey

Cisco IOS Software, Version 12.4(11)T, bietet zusätzliche Statistiken für eine einfachere Abstimmung des DoS-Schutzes.

Einige Funktionen der Cisco IOS Classic Firewall werden in Version 12.4(15)T der Cisco IOS Software in einer ZFW noch nicht unterstützt:

- Authentifizierungs-Proxy
- Stateful Firewall-Failover
- Einheitliche Firewall-MIB
- IPv6 Stateful Inspection
- Unterstützung von TCP-Out-of-Order

ZFW verbessert generell die Cisco IOS-Leistung für die meisten Firewall-Inspektionsaktivitäten. Weder Cisco IOS ZFW noch Classic Firewall bieten Unterstützung für Stateful Inspection für Multicast-Datenverkehr.

Zonenbasierte Richtlinien im Überblick

Die Stateful Inspection der Cisco IOS Classic Firewall (ehemals Context-Based Access Control, oder CBAC) stützte sich auf ein schnittstellenbasiertes Konfigurationsmodell, bei dem eine Stateful Inspection-Richtlinie auf eine Schnittstelle angewendet wurde. Der gesamte Datenverkehr, der diese Schnittstelle passiert, erhielt die gleiche Prüfrichtlinie. Dieses Konfigurationsmodell beschränkte die Genauigkeit der Firewall-Richtlinien und verursachte Verwirrung bei der ordnungsgemäßen Anwendung der Firewall-Richtlinien, insbesondere in Szenarien, in denen Firewall-Richtlinien zwischen mehreren Schnittstellen angewendet werden müssen.

Die zonenbasierte Richtlinien-Firewall (auch als zonenbasierte Firewall oder ZFW bezeichnet) ändert die Firewall-Konfiguration vom älteren schnittstellenbasierten Modell in ein flexibleres,

besser verständliches zonenbasiertes Modell. Schnittstellen werden Zonen zugewiesen, und Prüfrichtlinien werden auf Datenverkehr angewendet, der sich zwischen den Zonen bewegt. Zonenübergreifende Richtlinien bieten ein hohes Maß an Flexibilität und Präzision, sodass unterschiedliche Prüfrichtlinien auf mehrere, mit derselben Router-Schnittstelle verbundene Host-Gruppen angewendet werden können.

Firewall-Richtlinien werden mit der Cisco Policy Language (CPL) konfiguriert, die eine hierarchische Struktur verwendet, um die Überprüfung der Netzwerkprotokolle und der Gruppen von Hosts zu definieren, auf die die Überprüfung angewendet werden kann.

Zonenbasiertes Richtlinienkonfigurationsmodell

Die ZFW verändert die Konfiguration einer Cisco IOS Firewall-Inspektion komplett im Vergleich zur Cisco IOS Classic Firewall.

Die erste wichtige Änderung an der Firewall-Konfiguration ist die Einführung einer zonenbasierten Konfiguration. Die Cisco IOS Firewall ist die erste Funktion der Cisco IOS Software zum Schutz vor Bedrohungen, die ein Zonenkonfigurationsmodell implementiert. Andere Funktionen können das Zonenmodell im Laufe der Zeit übernehmen. Das schnittstellenbasierte Konfigurationsmodell der Cisco IOS Classic Firewall (CBAC), das den Befehlssatz ip inspect verwendet, wird über einen bestimmten Zeitraum beibehalten. Allerdings sind nur wenige neue Funktionen mit der klassischen Kommandozeile (CLI) konfigurierbar. Die Stateful Inspection- und CBAC-Befehle werden von der ZFW nicht verwendet. Die beiden Konfigurationsmodelle können gleichzeitig auf Routern verwendet werden, nicht jedoch kombiniert auf Schnittstellen. Eine Schnittstelle kann nicht als Mitglied einer Sicherheitszone konfiguriert und gleichzeitig für IP Inspect konfiguriert werden.

Zonen bilden die Sicherheitsgrenzen Ihres Netzwerks. Eine Zone definiert eine Grenze, an der der Datenverkehr bei der Übertragung in eine andere Region Ihres Netzwerks Richtlinien unterliegt. Die ZFW-Standardrichtlinie zwischen Zonen lautet "Alle verweigern". Wenn keine Richtlinie explizit konfiguriert wird, wird der gesamte Datenverkehr zwischen den Zonen blockiert. Dies bedeutet eine deutliche Abweichung vom Stateful Inspection-Modell, bei dem der Datenverkehr implizit zugelassen wurde, bis er explizit mit einer Zugriffskontrollliste (ACL) blockiert wurde.

Die zweite wichtige Änderung betrifft die Einführung einer neuen Richtliniensprache für die Konfiguration, die als CPL bezeichnet wird. Benutzer, die mit der Cisco IOS Software Modular Quality-of-Service (QoS) CLI (MQC) vertraut sind, erkennen, dass das Format der QoS-Verwendung von Klassenzuordnungen ähnelt, um anzugeben, welcher Datenverkehr von der in einer Richtlinienzuordnung angewendeten Aktion betroffen ist.

Regeln für zonenbasierte Firewall-Richtlinienanwendung

Die Zugehörigkeit zu einer Router-Netzwerkschnittstelle unterliegt verschiedenen Regeln, die das Verhalten der Schnittstelle regeln, ebenso wie der Datenverkehr zwischen den Schnittstellen der Zonenmitglieder:

- Bevor Schnittstellen der Zone zugewiesen werden können, muss eine Zone konfiguriert werden.
- Eine Schnittstelle kann nur einer Sicherheitszone zugewiesen werden.
- Sämtlicher Datenverkehr von und zu einer bestimmten Schnittstelle wird implizit blockiert, wenn die Schnittstelle einer Zone zugewiesen wird, mit Ausnahme des Datenverkehrs zu und

von anderen Schnittstellen in derselben Zone sowie des Datenverkehrs zu einer beliebigen Schnittstelle auf dem Router.
- Der Datenverkehr darf standardmäßig zwischen Schnittstellen fließen, die Mitglieder derselben Zone sind.
- Damit Datenverkehr von und zu einer Zonenelementschnittstelle zugelassen wird, muss zwischen dieser Zone und jeder anderen Zone eine Richtlinie konfiguriert werden, die Datenverkehr zulässt oder überprüft.
- Die Kernzone ist die einzige Ausnahme von der Standardrichtlinie "deny all". Der gesamte Datenverkehr zu einer beliebigen Router-Schnittstelle ist zulässig, bis der Datenverkehr explizit abgelehnt wird.
- Der Datenverkehr kann nicht zwischen einer Schnittstelle für Zonenelemente und einer Schnittstelle, die kein Zonenelement ist, übertragen werden. Aktionen zum Übergeben, Überprüfen und Verwerfen können nur zwischen zwei Zonen angewendet werden.
- Schnittstellen, die keiner Zone zugewiesen wurden, fungieren als klassische Router-Ports und können weiterhin die klassische Stateful Inspection-/CBAC-Konfiguration verwenden.
- Falls erforderlich, muss eine Schnittstelle auf dem Gerät nicht Teil der Zone-/Firewall-Richtlinie sein. Es kann weiterhin erforderlich sein, diese Schnittstelle in einer Zone zu platzieren und eine "pass all"-Richtlinie (eine Art Dummy-Richtlinie) zwischen dieser Zone und jeder anderen Zone zu konfigurieren, zu der der Datenverkehr fließen soll.
- Aus dem vorherigen Verhalten folgt, dass, wenn Datenverkehr zwischen allen Schnittstellen in einem Router fließen soll, alle Schnittstellen Teil des Zoning-Modells sein müssen (jede Schnittstelle muss Mitglied einer Zone oder einer anderen sein).
- Die einzige Ausnahme vom vorherigen Verhalten, deny per default (Standard verweigern), ist der Datenverkehr zum und vom Router, der standardmäßig zulässig ist. Eine explizite Richtlinie kann konfiguriert werden, um diesen Datenverkehr zu beschränken.

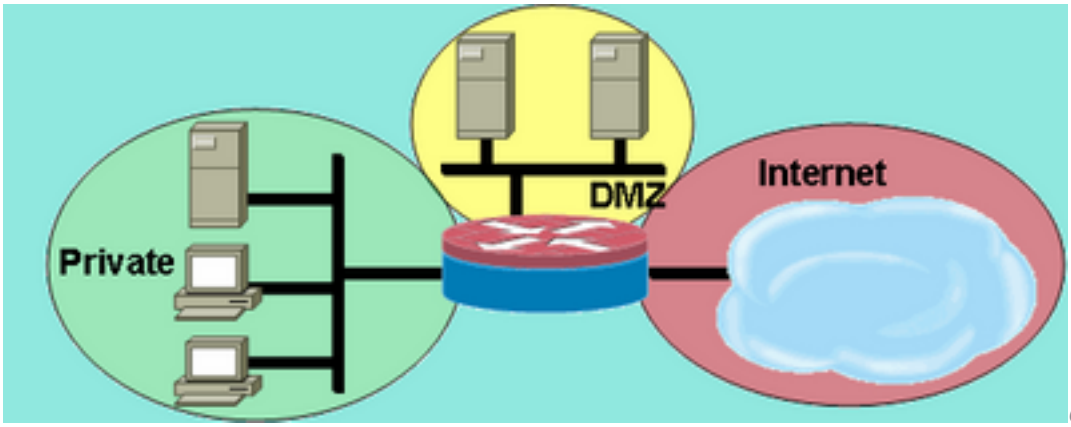
Netzwerksicherheit mit zonenbasierten Richtlinien

Für jede Region der relativen Sicherheit im Netzwerk muss eine Sicherheitszone konfiguriert werden, damit alle Schnittstellen, die derselben Zone zugewiesen sind, mit einem ähnlichen Sicherheitsniveau geschützt sind. Stellen Sie sich beispielsweise einen Access-Router mit drei Schnittstellen vor:

- Eine mit dem öffentlichen Internet verbundene Schnittstelle
- Eine Schnittstelle, die mit einem privaten LAN verbunden ist und nicht vom öffentlichen Internet aus zugänglich sein darf
- Eine Schnittstelle, die mit einer demilitarisierten Zone (DMZ) für den Internetdienst verbunden ist, in der ein Webserver, ein DNS- (Domain Name System) Server und ein E-Mail-Server für das öffentliche Internet zugänglich sein müssen

Jede Schnittstelle in diesem Netzwerk ist einer eigenen Zone zugewiesen. Sie können jedoch einen unterschiedlichen Zugriff vom öffentlichen Internet auf bestimmte Hosts in der DMZ und verschiedene Anwendungsnutzungsrichtlinien für Hosts im geschützten LAN zulassen (siehe Abbildung 1).

Abbildung 1: Grundlegende Topologie der Sicherheitszonen



Grundlegende Topologie der Sicherheitszonen

In diesem Beispiel enthält jede Zone nur eine Schnittstelle. Wenn der privaten Zone eine zusätzliche Schnittstelle hinzugefügt wird, können die Hosts, die mit der neuen Schnittstelle in der Zone verbunden sind, Datenverkehr an alle Hosts der aktuellen Schnittstelle in derselben Zone weiterleiten. Außerdem wird der Host-Datenverkehr zu Hosts in anderen Zonen durch die aktuellen Richtlinien ebenfalls beeinflusst.

In der Regel weist das Beispielnetzwerk drei Hauptrichtlinien auf:

- Verbindung der privaten Zone mit dem Internet
- Verbindung zur privaten Zone mit DMZ-Hosts
- Verbindung mit der Internetzone zu DMZ-Hosts

Da die DMZ dem öffentlichen Internet ausgesetzt ist, können die DMZ-Hosts unerwünschten Aktivitäten von böswilligen Personen ausgesetzt sein, die einen oder mehrere DMZ-Hosts beschädigen können. Wenn keine Zugriffsrichtlinie für DMZ-Hosts bereitgestellt wird, um entweder Hosts in der privaten Zone oder in der Internet-Zone zu erreichen, können die Personen, die die DMZ-Hosts kompromittiert haben, die DMZ-Hosts nicht für weitere Angriffe auf private oder Internet-Hosts verwenden. Die ZFW hat einen prohibitiven Standard-Sicherheitsstatus. Sofern den DMZ-Hosts nicht ausdrücklich Zugriff auf andere Netzwerke gewährt wird, sind andere Netzwerke gegen Verbindungen von den DMZ-Hosts geschützt. Ebenso wird für Internet-Hosts kein Zugriff auf die privaten Zonenhosts bereitgestellt, sodass private Zonenhosts vor unerwünschtem Zugriff durch Internet-Hosts geschützt sind.

Verwendung von IPSec VPN mit zonenbasierter Richtlinien-Firewall

Kürzlich erfolgte Erweiterungen des IPSec VPN vereinfachen die Konfiguration von Firewall-Richtlinien für VPN-Verbindungen. IPSec Virtual Tunnel Interface (VTI) und GRE+IPSec ermöglichen die Beschränkung von standortübergreifenden VPN- und Client-Verbindungen auf eine bestimmte Sicherheitszone durch die Platzierung der Tunnelschnittstellen in einer bestimmten Sicherheitszone. Verbindungen können in einer VPN-DMZ isoliert werden, wenn die Verbindung durch eine bestimmte Richtlinie eingeschränkt werden muss. Wenn die VPN-Verbindung implizit vertrauenswürdig ist, kann die VPN-Verbindung in derselben Sicherheitszone wie das vertrauenswürdige interne Netzwerk angeordnet werden.

Wird ein Nicht-VTI-IPSec angewendet, muss die Firewall-Richtlinie für die VPN-Konnektivität aus Sicherheitsgründen genau geprüft werden. Die Zonenrichtlinie muss speziell den Zugriff durch eine IP-Adresse für Hosts an Remote-Standorten oder VPN-Clients zulassen, wenn sich sichere Hosts in einer anderen Zone befinden als die mit dem VPN-Client verschlüsselte Verbindung zum

Router. Wenn die Zugriffsrichtlinie nicht richtig konfiguriert ist, können Hosts, die geschützt werden müssen, unerwünschten, potenziell feindlichen Hosts ausgesetzt sein. Weitere Konzepte und Konfigurationen finden Sie unter Verwenden von VPN mit zonenbasierter Richtlinien-Firewall.

Konfiguration der Cisco Policy Language (CPL)

Mit diesem Verfahren kann eine ZFW konfiguriert werden. Die Reihenfolge der Schritte ist nicht wichtig, aber einige Ereignisse müssen der Reihe nach abgeschlossen werden. Sie müssen beispielsweise eine Klassenzuordnung konfigurieren, bevor Sie einer Richtlinienzuordnung eine Klassenzuordnung zuweisen. Ebenso können Sie einem Zonenpaar erst eine Richtlinienzuordnung zuweisen, wenn Sie die Richtlinie konfiguriert haben. Wenn Sie versuchen, einen Abschnitt zu konfigurieren, der auf einem anderen Teil der Konfiguration basiert, den Sie nicht konfiguriert haben, antwortet der Router mit einer Fehlermeldung.

1. Definieren Sie Zonen.
2. Definieren Sie Zonenpaare.
3. Definieren Sie Klassenzuordnungen, die den Datenverkehr beschreiben, für den Richtlinien angewendet werden müssen, wenn er ein Zonenpaar kreuzt.
4. Definieren Sie Richtlinienzuordnungen, um Aktionen auf den Klassenzuordnungsverkehr anzuwenden.
5. Wenden Sie Richtlinienzuordnungen auf Zonenpaare an.
6. Zuweisen von Schnittstellen zu Zonen

Konfigurieren zonenbasierter Richtlinien Firewall-Klassenzuordnungen

Klassenzuordnungen definieren den Datenverkehr, den die Firewall für die Richtlinienanwendung auswählt. Durch Layer-4-Klassenzuordnungen wird der Datenverkehr anhand der hier aufgeführten Kriterien sortiert. Diese Kriterien werden mit dem Befehl match in einer Klassenzuordnung angegeben:

- Zugriffsgruppe - Eine standardisierte, erweiterte oder benannte ACL kann den Datenverkehr basierend auf der Quell- und Ziel-IP-Adresse sowie dem Quell- und Ziel-Port filtern.
- Protokoll - Die Layer-4-Protokolle (TCP, UDP und ICMP) und Anwendungsdienste wie HTTP, SMTP, DNS usw. Jeder bekannte oder benutzerdefinierte Dienst, der der Port-Anwendungszuordnung bekannt ist, kann angegeben werden.
- Klassenzuordnung - Eine untergeordnete Klassenzuordnung, die zusätzliche Anpassungskriterien bereitstellt, kann in eine andere Klassenzuordnung geschachtelt werden.
- Not (Nicht): Das "not"-Kriterium gibt an, dass Datenverkehr, der nicht mit einem bestimmten Service (Protokoll), einer Zugriffsgruppe oder einer untergeordneten Klassenzuordnung übereinstimmt, für die Klassenzuordnung ausgewählt wird.

Kombinieren Sie "Zuordnungskriterien": "Match-Any" und "Match-All"

Mithilfe von Klassenzuordnungen können beliebige oder alle übereinstimmende Operatoren angewendet werden, um zu bestimmen, wie die übereinstimmenden Kriterien angewendet werden. Wenn match-any angegeben ist, darf der Datenverkehr nur eines der Übereinstimmungskriterien in der Klassenzuordnung erfüllen. Wenn match-all angegeben ist, muss der Datenverkehr alle Klassenzuordnungskriterien erfüllen, um zu dieser bestimmten Klasse zu gehören.

Übereinstimmungskriterien müssen in der Reihenfolge von spezifischer zu weniger spezifisch angewendet werden, wenn der Datenverkehr mehrere Kriterien erfüllt. Betrachten Sie beispielsweise diese Klassenzuordnung:

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

Der HTTP-Datenverkehr muss zuerst auf das Match-Protokoll http treffen, um sicherzustellen, dass der Datenverkehr von den dienstspezifischen Funktionen der HTTP-Überprüfung verarbeitet wird. Wenn die Übereinstimmungslinien umgekehrt werden, sodass der Datenverkehr auf die TCP-Anweisung des Übereinstimmungsprotokolls trifft, bevor er sie mit dem HTTP-Protokoll vergleicht, wird der Datenverkehr einfach als TCP-Datenverkehr klassifiziert und anhand der Funktionen der TCP-Überprüfungskomponente der Firewall überprüft. Dies ist ein Problem für bestimmte Dienste wie FTP, TFTP und mehrere Multimedia- und Sprachsignalisierungsdienste wie H.323, SIP, Skinny, RTSP und andere. Diese Services erfordern zusätzliche Prüfungsfunktionen, um die komplexeren Aktivitäten dieser Services zu erkennen.

Anwenden einer ACL als Zuordnungskriterien

Klassenzuordnungen können eine ACL als eines der Abgleichskriterien für die Richtlinienanwendung anwenden. Wenn eine Klassenzuordnung nur das Kriterium einer ACL erfüllt und die Klassenzuordnung mit einer Richtlinienzuordnung verknüpft ist, die die Aktion "inspect" anwendet, wendet der Router eine grundlegende TCP- oder UDP-Überprüfung für den gesamten von der ACL zulässigen Datenverkehr an, mit Ausnahme des Datenverkehrs, der von der ZFW anwendungssensitiv geprüft wird. Dazu gehören (aber nicht beschränkt auf) FTP, SIP, Skinny (SCCP), H.323, Sun RPC und TFTP. Wenn eine anwendungsspezifische Überprüfung verfügbar ist und die ACL den primären oder Steuerungskanal zulässt, sind alle mit dem primären/Steuerungskanal verbundenen sekundären oder Medienkanäle zulässig, unabhängig davon, ob die ACL den Datenverkehr zulässt.

Wenn eine Klassenzuordnung nur die ACL 101 als Abgleichskriterien anwendet, wird eine ACL 101 wie folgt angezeigt:

```
access-list 101 permit ip any any
```

Der gesamte Datenverkehr wird in Richtung der auf ein bestimmtes Zonenpaar angewendeten Dienstrichtlinie zugelassen, und der entsprechende zurückkehrende Datenverkehr wird in die entgegengesetzte Richtung zugelassen. Daher muss die ACL die Einschränkung anwenden, um den Datenverkehr auf bestimmte gewünschte Typen zu beschränken. Beachten Sie, dass die PAM-Liste Anwendungsdienste wie HTTP, NetBIOS, H.323 und DNS enthält. Obwohl PAM die spezifische Anwendungsnutzung eines bestimmten Ports kennt, wendet die Firewall nur ausreichend anwendungsspezifische Funktionen an, um die bekannten Anforderungen des Anwendungsdatenverkehrs zu erfüllen. So wird einfacher Anwendungsdatenverkehr wie Telnet, SSH und andere Single-Channel-Anwendungen als TCP überprüft, und ihre Statistiken werden in der Ausgabe des Befehls show zusammengefasst. Wenn eine anwendungsspezifische Transparenz der Netzwerkaktivität gewünscht wird, müssen Sie die Überprüfung der Services anhand des Anwendungsnamens konfigurieren (Konfiguration des Übereinstimmungsprotokolls HTTP, Übereinstimmungsprotokoll Telnet usw.).

Vergleichen Sie die Statistiken, die in der Ausgabe des Befehls show policy-map type inspect zone-pair aus dieser Konfiguration verfügbar sind, mit der detaillierteren Firewall-Richtlinie, die weiter unten auf der Seite angezeigt wird. Mit dieser Konfiguration wird der Datenverkehr von

einem Cisco IP-Telefon sowie von mehreren Workstations geprüft, die unterschiedliche Datenverkehrsarten verwenden, darunter HTTP, FTP, NetBIOS, SSH und DNS:

```
class-map type inspect match-all all-private
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect all-private
  inspect
 class class-default
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

Diese Konfiguration ist einfach zu definieren und berücksichtigt den gesamten Datenverkehr, der aus der privaten Zone stammt (solange der Datenverkehr die standardmäßigen, von PAM erkannten Ziel-Ports beachtet). Sie bietet jedoch nur eine begrenzte Transparenz der Service-Aktivitäten und keine Möglichkeit, die Bandbreite und Sitzungslimits von ZFW für bestimmte Datenverkehrstypen anzuwenden. Diese Ausgabe des Befehls show policy-map type inspect zone-pair priv-pub ist das Ergebnis der vorherigen einfachen Konfiguration, die nur eine Zulassen-IP [Subnetz] und eine ACL zwischen Zonenpaaren verwendet. Wie Sie sehen, wird der Großteil des Workstation-Datenverkehrs in den grundlegenden TCP- oder UDP-Statistiken gezählt:

```
stg-871-L#show policy-map type insp zone-pair priv-pub
Zone-pair: priv-pub

  Service-policy inspect : priv-pub-pmap

    Class-map: all-private (match-all)
      Match: access-group 101
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [413:51589]
        udp packets: [74:28]
        icmp packets: [0:8]
        ftp packets: [23:0]
        tftp packets: [3:0]
        tftp-data packets: [6:28]
        skinny packets: [238:0]

        Session creations since subsystem startup or last reset 39
        Current session counts (estab/half-open/terminating) [3:0:0]
        Maxever session counts (estab/half-open/terminating) [3:4:1]
        Last session created 00:00:20
        Last statistic reset never
        Last session creation rate 2
        Maxever session creation rate 7
        Last half-open session total 0
```

```
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Eine ähnliche Konfiguration, die anwendungsspezifische Klassen hinzufügt, bietet dagegen detailliertere Anwendungsstatistiken und eine bessere Kontrolle und berücksichtigt dennoch dieselbe Bandbreite an Services, die im ersten Beispiel gezeigt wurde, als Sie die Klassenzuordnung der letzten Chance definieren, die nur mit der ACL als letzte Chance in der Richtlinienzuordnung übereinstimmt:

```
class-map type inspect match-all all-private
 match access-group 101
class-map type inspect match-all private-ftp
 match protocol ftp
 match access-group 101
class-map type inspect match-any netbios
 match protocol msrpc
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
class-map type inspect match-all private-netbios
 match class-map netbios
 match access-group 101
class-map type inspect match-all private-ssh
 match protocol ssh
 match access-group 101
class-map type inspect match-all private-http
 match protocol http
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect private-http
  inspect
 class type inspect private-ftp
  inspect
 class type inspect private-ssh
  inspect
 class type inspect private-netbios
  inspect
 class type inspect all-private
  inspect
 class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

Die spezifischere Konfiguration bietet diese umfassende, detaillierte Ausgabe für den Befehl show policy-map type inspect zone-pair priv-pub:

```
stg-871-L#sh policy-map type insp zone-pair priv-pub
 Zone-pair: priv-pub

   Service-policy inspect : priv-pub-pmap

     Class-map: private-http (match-all)
       Match: protocol http
       Match: access-group 101
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:2193]

         Session creations since subsystem startup or last reset 731
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [0:3:0]
         Last session created 00:29:25
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 4
         Last half-open session total 0

     Class-map: private-ftp (match-all)
       Match: protocol ftp
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [86:167400]
         ftp packets: [43:0]

         Session creations since subsystem startup or last reset 7
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [2:1:1]
         Last session created 00:42:49
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 4
         Last half-open session total 0

     Class-map: private-ssh (match-all)
       Match: protocol ssh
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:62]

         Session creations since subsystem startup or last reset 4
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [1:1:1]
         Last session created 00:34:18
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 2
         Last half-open session total 0

     Class-map: private-netbios (match-all)
       Match: access-group 101
       Match: class-map match-any netbios
         Match: protocol msrpc
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: protocol netbios-dgm
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: protocol netbios-ns
```

```
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol netbios-ssn
        2 packets, 56 bytes
        30 second rate 0 bps
    Inspect
      Packet inspection statistics [process switch:fast switch]
      tcp packets: [0:236]

      Session creations since subsystem startup or last reset 2
      Current session counts (estab/half-open/terminating) [0:0:0]
      Maxever session counts (estab/half-open/terminating) [1:1:1]
      Last session created 00:31:32
      Last statistic reset never
      Last session creation rate 0
      Maxever session creation rate 1
      Last half-open session total 0

  Class-map: all-private (match-all)
    Match: access-group 101
    Inspect
      Packet inspection statistics [process switch:fast switch]
      tcp packets: [51725:158156]
      udp packets: [8800:70]
      tftp packets: [8:0]
      tftp-data packets: [15:70]
      skinny packets: [33791:0]

      Session creations since subsystem startup or last reset 2759
      Current session counts (estab/half-open/terminating) [2:0:0]
      Maxever session counts (estab/half-open/terminating) [2:6:1]
      Last session created 00:22:21
      Last statistic reset never
      Last session creation rate 0
      Maxever session creation rate 12
      Last half-open session total 0

  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      4 packets, 112 bytes
```

Ein weiterer Vorteil bei Verwendung einer detaillierteren Klassenzuordnungs- und Richtlinienzuordnungskonfiguration besteht, wie bereits erwähnt, in der Möglichkeit, klassenspezifische Beschränkungen für Sitzungs- und Ratenwerte anzuwenden. und zur gezielten Anpassung von Prüfparametern durch die Anwendung einer Parameterzuordnung zur Anpassung des Prüfverhaltens jeder Klasse.

Konfigurieren einer zonenbasierten Richtlinie Firewall-Richtlinienzuordnungen

Die Richtlinienzuordnung wendet Firewall-Richtlinienaktionen auf eine oder mehrere Klassenzuordnungen an, um die Dienstrichtlinie zu definieren, die auf ein Sicherheitszonenpaar angewendet wird. Wenn eine inspect-type policy-map erstellt wird, wird am Ende der Klasse die Standardklasse class class-default angewendet. Die Standardrichtlinienaktion "class-default" lautet "drop", kann aber geändert werden, um sie zu bestehen. Die Protokolloption kann mit der Dropdown-Aktion hinzugefügt werden. Inspect kann nicht auf den Klassenstandardwert angewendet werden.

Firewall-Aktionen mit zonenbasierten Richtlinien

Die ZFW bietet drei Aktionen für Datenverkehr, der zwischen Zonen übertragen wird:

- Drop (Löschen) - Dies ist die Standardaktion für den gesamten Datenverkehr. Sie wird von der class-default angewendet, die jede inspect-type policy-map beendet. Andere Klassenzuordnungen innerhalb einer Richtlinienzuweisung können ebenfalls so konfiguriert werden, dass unerwünschter Datenverkehr verworfen wird. Datenverkehr, der von der Drop-Aktion verarbeitet wird, wird von der ZFW stillschweigend verworfen (d. h., es wird keine Benachrichtigung über den Verfall an den relevanten End-Host gesendet), im Gegensatz zu einem ACL-Verhalten, wenn eine ICMP-Meldung "host unreachable" an den Host gesendet wird, der den abgelehnten Datenverkehr gesendet hat. Derzeit besteht keine Möglichkeit, das Silent-Drop-Verhalten zu ändern. Die Protokolloption kann mit drop für eine Syslog-Benachrichtigung hinzugefügt werden, dass der Datenverkehr von der Firewall fallen gelassen wurde.
- Pass (Übergeben) - Mit dieser Aktion kann der Router Datenverkehr von einer Zone an eine andere weiterleiten. Die Aktion "pass" verfolgt den Status von Verbindungen oder Sitzungen im Datenverkehr nicht. Beim Pass wird der Verkehr nur in eine Richtung zugelassen. Es muss eine Parallelrichtlinie angewendet werden, um den umgekehrten Datenverkehr zuzulassen. Die Aktion "pass" ist für Protokolle wie IPSec ESP, IPSec AH, ISAKMP und andere per se sichere Protokolle mit vorhersagbarem Verhalten nützlich. Der Großteil des Anwendungsdatenverkehrs wird jedoch mit der Aktion "inspect" besser in der ZFW verarbeitet.
- Inspizieren - Die Aktion "Inspizieren" ermöglicht eine zustandsbasierte Datenverkehrskontrolle. Wenn beispielsweise der Datenverkehr von der privaten Zone zur Internetzone im Netzwerk des vorherigen Beispiels überprüft wird, erhält der Router Verbindungs- oder Sitzungsinformationen für TCP- und UDP-Datenverkehr (User Datagram Protocol). Daher lässt der Router den Rückverkehr zu, der von den Hosts der Internetzone als Antwort auf Verbindungsanforderungen für die private Zone gesendet wird. Darüber hinaus kann Inspection eine Anwendungsprüfung und -kontrolle für bestimmte Serviceprotokolle bereitstellen, die anfälligen oder sensiblen Anwendungsdatenverkehr übertragen können. Audit-Trail kann mit einer Parameterzuordnung angewendet werden, um Verbindungs-/Sitzungsstart, Stopp, Dauer, das übertragene Datenvolumen sowie Quell- und Zieladressen aufzuzeichnen.

Aktionen sind Klassenzuordnungen in Richtlinienzuordnungen zugeordnet:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Parameter-Maps bieten Optionen zum Ändern der Verbindungsparameter für eine bestimmte Klassenzuweisungsrichtlinie.

Konfigurieren von Parameterzuordnungen für die Firewall nach Zonenrichtlinien

Parameterzuordnungen definieren das Prüfverhalten für ZFW, für Parameter wie DoS-Schutz, TCP-Verbindungs-/UDP-Sitzungs-Timer und die Einrichtung der Prüfpfadprotokollierung. Parameterzuordnungen werden auch mit Layer-7-Klassen- und Richtlinienzuordnungen angewendet, um anwendungsspezifisches Verhalten wie HTTP-Objekte, POP3- und IMAP-Authentifizierungsanforderungen und andere anwendungsspezifische Informationen zu definieren.

Inspection Parameter-Maps für ZFW werden ähnlich wie andere ZFW Klassen und Policy-Objekte als Type Inspect konfiguriert:

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#?
parameter-map commands:
  alert           Turn on/off alert
  audit-trail     Turn on/off audit trail
  dns-timeout     Specify timeout for DNS
  exit            Exit from parameter-map
  icmp            Config timeout values for icmp
  max-incomplete  Specify maximum number of incomplete connections before
                  clamping
  no              Negate or set default values of a command
  one-minute      Specify one-minute-sample watermarks for clamping
  sessions        Maximum number of inspect sessions
  tcp             Config timeout values for tcp connections
  udp             Config timeout values for udp flows
```

Bestimmte Arten von Parameterzuordnungen geben Parameter an, die von Layer-7-Anwendungsinspektionsrichtlinien angewendet werden. Parameterzuordnungen vom Regex-Typ definieren einen regulären Ausdruck für die HTTP-Anwendungsüberprüfung, der den Datenverkehr mit einem regulären Ausdruck filtert:

```
parameter-map type regex [parameter-map-name]
```

Protocol-Info-Type Parameter-Maps definieren Servernamen für die IM-Anwendungsüberprüfung:

```
parameter-map type protocol-info [parameter-map-name]
```

Vollständige Konfigurationsdetails für die HTTP- und IM-Anwendungsinspektion finden Sie in den entsprechenden Abschnitten zur Anwendungsinspektion dieses Dokuments.

Protokollierung für zonenbasierte Firewall-Richtlinien anwenden

ZFW bietet Protokollierungsoptionen für Datenverkehr, der durch standardmäßige oder konfigurierte Firewall-Richtlinienaktionen verworfen oder überprüft wird. Für den von der ZFW untersuchten Verkehr steht die Audit-Trail-Protokollierung zur Verfügung. Audit-trail wird angewendet, wenn ein Audit-Trail in einer Parameter-Map und die Parameter-Map mit der Aktion inspect in einer Policy-Map definiert ist:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

Drop-Logging ist für den Verkehr verfügbar, den die ZFW verwirft. Die Drop-Protokollierung wird konfiguriert, wenn Sie ein Protokoll mit der Drop-Aktion in einer Richtlinienzuordnung hinzufügen:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Klassenzuordnungen und Richtlinienzuordnungen für die Zonenrichtlinien-Firewall bearbeiten

Die ZFW verfügt derzeit nicht über einen Editor, der die verschiedenen ZFW-Strukturen wie Richtlinienzuordnungen, Klassenzuordnungen und Parameterzuordnungen verändern kann. Um Zuordnungsanweisungen in einer Klassenzuordnung oder einer Aktionsanwendung in verschiedene Klassenzuordnungen in einer Richtlinienzuordnung umzuordnen, müssen Sie die folgenden Schritte ausführen:

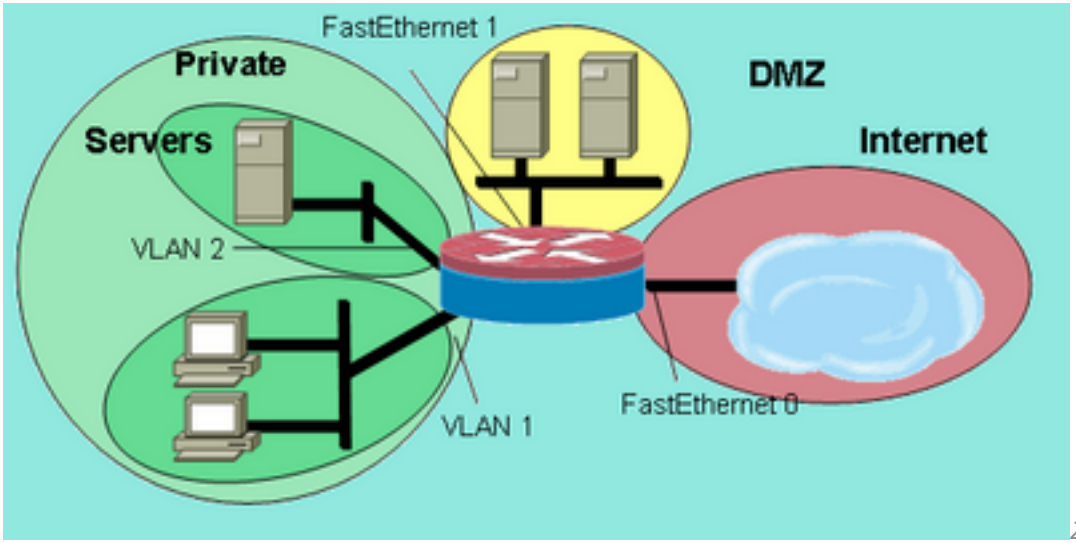
1. Kopieren Sie die aktuelle Struktur in einen Text-Editor wie Microsoft Windows Editor oder einen Editor wie vi auf Linux/Unix-Plattformen.
2. Entfernen Sie die aktuelle Struktur aus der Routerkonfiguration.
3. Bearbeiten Sie die Struktur in Ihrem Texteditor.
4. Kopieren Sie die Struktur zurück in die Router-CLI.

Konfigurationsbeispiele

In diesem Konfigurationsbeispiel wird ein Cisco 1811 Integrated Services Router verwendet. Anhang A enthält eine Basiskonfiguration mit IP-Verbindungen, VLAN-Konfiguration und transparentem Bridging zwischen zwei privaten Ethernet-LAN-Segmenten. Der Router ist in fünf Zonen unterteilt:

- Das öffentliche Internet ist mit FastEthernet 0 (Internetzone) verbunden.
- FastEthernet 1 (DMZ-Zone) ist mit zwei Internet-Servern verbunden
- Der Ethernet-Switch wird mit zwei VLANs konfiguriert:Workstations sind mit VLAN1 (Client-Zone) verbunden.Server werden mit VLAN2 (Serverzone) verbunden.Die Client- und Serverzonen befinden sich im gleichen Subnetz. Zwischen den Zonen wird eine transparente Firewall angewendet, sodass sich die zonenübergreifenden Richtlinien auf diesen beiden Schnittstellen nur auf den Datenverkehr zwischen der Client- und Serverzone auswirken können.
- Die Schnittstellen VLAN1 und VLAN2 kommunizieren über die virtuelle Bridge-Schnittstelle (BVI1) mit anderen Netzwerken. Diese Schnittstelle wird der privaten Zone zugewiesen. (Siehe Abbildung 2.)

Abbildung 2: Zonentopologie - Details

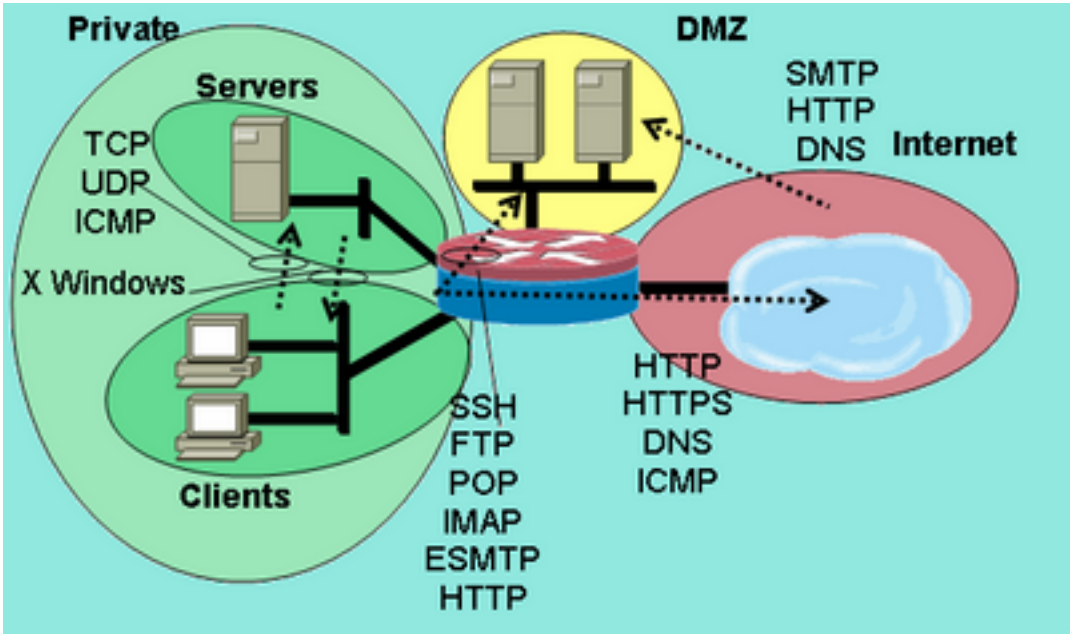


Zonentopologie - Details

Diese Richtlinien werden mit den zuvor definierten Netzwerkzonen angewendet:

- Hosts in der Internetzone können DNS-, SMTP- und SSH-Dienste auf einem Server in der DMZ erreichen. Der andere Server bietet SMTP-, HTTP- und HTTPS-Dienste. Die Firewall-Richtlinie schränkt den Zugriff auf die spezifischen Dienste ein, die auf jedem Host verfügbar sind.
- Die DMZ-Hosts können keine Verbindung zu Hosts in anderen Zonen herstellen.
- Hosts in der Clientzone können sich mit Hosts in der Serverzone über alle TCP-, UDP- und ICMP-Dienste verbinden.
- Hosts in der Serverzone können keine Verbindung zu Hosts in der Clientzone herstellen, außer ein UNIX-basierter Anwendungsserver kann X Windows-Clientsitzungen zu X Windows-Servern auf Desktop-PCs in der Clientzone auf den Ports 6900 bis 6910 öffnen.
- Alle Hosts in der privaten Zone (eine Kombination aus Clients und Servern) können auf Hosts in der DMZ mit SSH-, FTP-, POP-, IMAP-, ESMTP- und HTTP-Services zugreifen, und in der Internetzone mit HTTP-, HTTPS- und DNS-Services sowie ICMP. Darüber hinaus wird eine Anwendungsprüfung für HTTP-Verbindungen von der privaten Zone zur Internet-Zone durchgeführt, um sicherzustellen, dass unterstützte IM- und P2P-Anwendungen nicht auf Port 80 ausgeführt werden (siehe Abbildung 3).

Abbildung 3: Im Konfigurationsbeispiel anzuwendende Zone-Pair-Dienstberechtigungen



Im Konfigurationsbeispiel anzuwendende Zone-Pair-Dienstberechtigungen

Die Firewall-Richtlinien werden in der Reihenfolge ihrer Komplexität konfiguriert:

1. Clients-Server TCP/UDP/ICMP-Prüfung
2. Private-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP-Inspektion
3. Internet - DMZ SMTP/HTTP/DNS-Prüfung durch Hostadresse eingeschränkt
4. Server-Clients X Windows-Inspektion mit einem durch Port-Anwendungszuordnung (PAM) spezifizierten Service
5. HTTP/HTTPS/DNS/ICMP mit HTTP-Anwendungsinspektion

Da Sie Teile der Konfiguration zu unterschiedlichen Zeiten auf verschiedene Netzwerksegmente anwenden, ist es wichtig, darauf hinzuweisen, dass ein Netzwerksegment die Verbindung zu anderen Segmenten verliert, wenn es in einer Zone angeordnet wird. Wenn beispielsweise die private Zone konfiguriert ist, verlieren Hosts in der privaten Zone die Verbindung zur DMZ und den

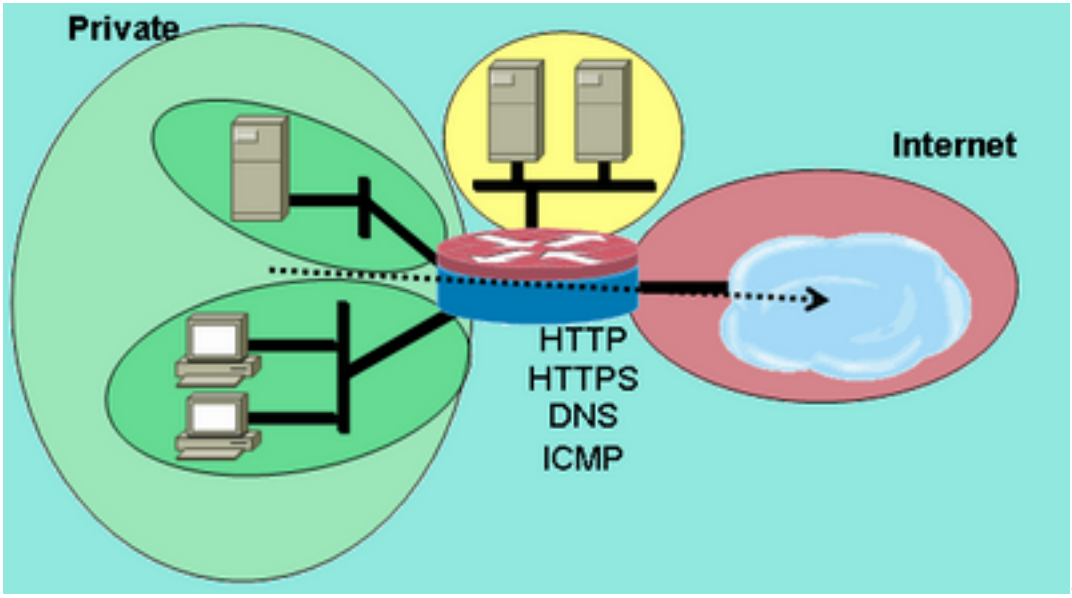
Internetzonen, bis die entsprechenden Richtlinien definiert sind.

Stateful Inspection Routing Firewall

Private Internetrichtlinie konfigurieren

Abbildung 4 zeigt die Konfiguration der privaten Internetrichtlinie.

Abbildung 4: Service-Inspektion von der privaten Zone zur Internet-Zone



Service-Inspektion von der privaten Zone zur Internet-Zone

Die private Internetrichtlinie wendet die Layer-4-Inspektion von der privaten Zone auf die HTTP-, HTTPS-, DNS- und Layer-4-Inspektion für ICMP an. Dies ermöglicht Verbindungen von der privaten Zone zur Internet-Zone und den zurückkehrenden Verkehr. Die Layer-7-Inspektion bietet die Vorteile einer strengeren Anwendungskontrolle, höherer Sicherheit und Unterstützung für Anwendungen, die eine Reparatur erfordern. Die Layer-7-Inspektion erfordert jedoch, wie erwähnt, ein besseres Verständnis der Netzwerkaktivität, da Layer-7-Protokolle, die nicht für die Inspektion konfiguriert sind, zwischen den Zonen nicht zulässig sind.

1. Definieren Sie Klassenzuordnungen, die den Datenverkehr zwischen Zonen beschreiben, den Sie auf der Grundlage der weiter oben beschriebenen Richtlinien zulassen möchten:
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Konfigurieren Sie eine Richtlinienzuweisung, um den Datenverkehr auf den gerade definierten Klassenzuweisungen zu überprüfen:
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Konfigurieren Sie die private Zone und die Internetzone, und weisen Sie den jeweiligen Zonen Router-Schnittstellen zu:
```
configure terminal
 zone security private
```

```
zone security internet
int bvi1
 zone-member security private
int fastethernet 0
 zone-member security internet
```

Konfigurieren Sie das Zonenpaar, und wenden Sie die entsprechende Richtlinienzuweisung an.

> **Anmerkung:** Sie müssen zur Zeit nur das private Internet-Zonenpaar konfigurieren, um die Verbindungen zu überprüfen, die von der privaten Zone stammen, die in die Internet-Zone übertragen wird (siehe nächstes Beispiel):

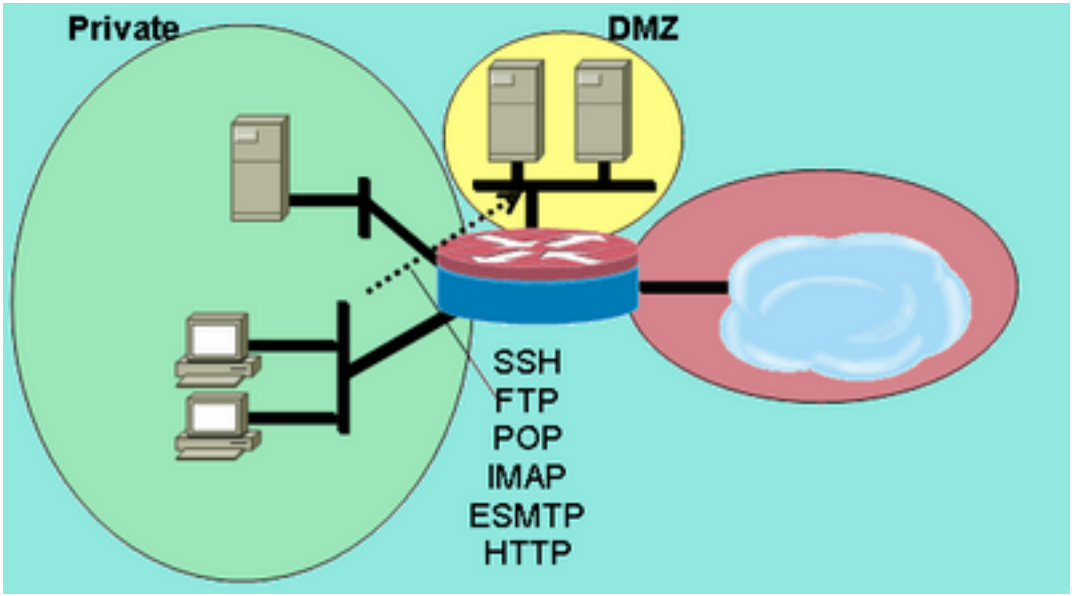
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

Damit ist die Konfiguration der Layer-7-Prüfrichtlinie für das private Internet-Zonenpaar abgeschlossen, damit HTTP-, HTTPS-, DNS- und ICMP-Verbindungen von der Client-Zone zur Server-Zone zugelassen werden und Anwendungsinspektion auf HTTP-Verkehr angewendet wird, um sicherzustellen, dass unerwünschter Verkehr nicht über TCP 80, den HTTP-Service-Port, übertragen werden darf.

Konfigurieren einer privaten DMZ-Richtlinie

Abbildung 5 zeigt die Konfiguration der privaten DMZ-Richtlinie.

Abbildung 5: Service-Inspektion von der privaten Zone zur DMZ



Service-Inspektion von der privaten Zone zur DMZ

Die Richtlinie für private DMZ erhöht die Komplexität, da sie ein besseres Verständnis des Netzwerkverkehrs zwischen den Zonen erfordert. Diese Richtlinie wendet die Layer-7-Inspektion von der privaten Zone auf die DMZ an. Dies ermöglicht Verbindungen von der privaten Zone zur DMZ und den zurückkehrenden Datenverkehr. Die Layer-7-Inspektion bietet die Vorteile einer strengeren Anwendungskontrolle, höherer Sicherheit und Unterstützung für Anwendungen, die eine Reparatur erfordern. Die Layer-7-Inspektion erfordert jedoch, wie erwähnt, ein besseres Verständnis der Netzwerkaktivität, da Layer-7-Protokolle, die nicht für die Inspektion konfiguriert sind, zwischen den Zonen nicht zulässig sind.

1. Definieren Sie Klassenzuordnungen, die den Datenverkehr zwischen Zonen beschreiben, den Sie auf der Grundlage der weiter oben beschriebenen Richtlinien zulassen möchten:
```
configure terminal
 class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
```
2. Konfigurieren Sie Richtlinienzuordnungen, um den Datenverkehr anhand der gerade definierten Klassenzuordnungen zu überprüfen:
```
configure terminal
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```
3. Konfigurieren Sie die private und die DMZ-Zone, und weisen Sie den jeweiligen Zonen Router-Schnittstellen zu:
```
configure terminal
 zone security private
 zone security dmz
 int bvi1
  zone-member security private
 int fastethernet 1
  zone-member security dmz
```
4. Konfigurieren Sie das Zonenpaar, und wenden Sie die entsprechende Richtlinienzuweisung an.

   Anmerkung: Sie müssen derzeit nur das private DMZ-Zonenpaar konfigurieren, um die Verbindungen zu überprüfen, die von der privaten Zone stammen, die zur DMZ geleitet wird (siehe folgende Abbildung):

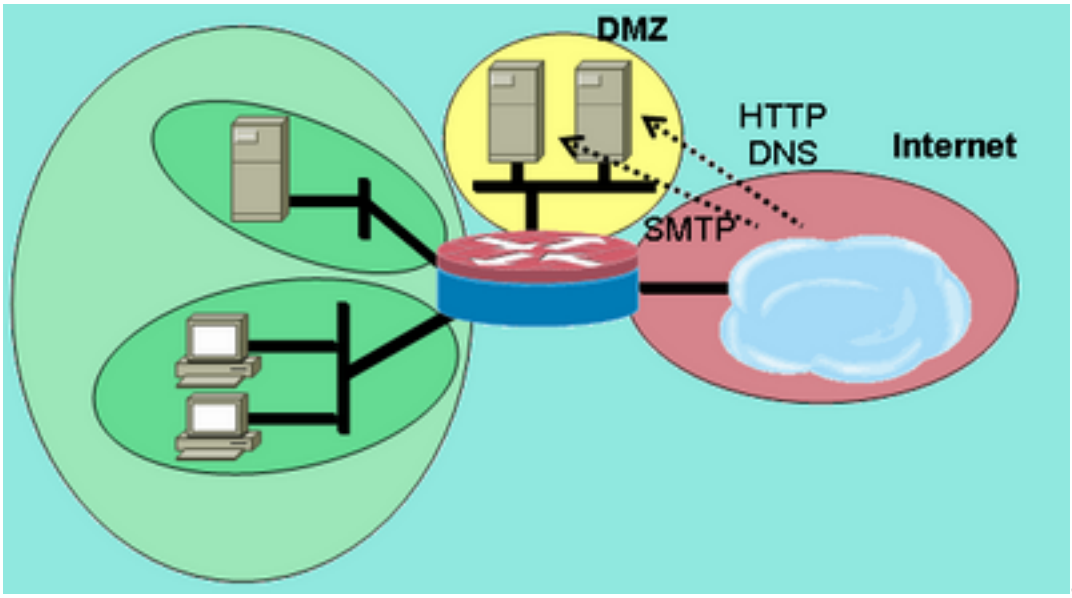
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

Damit ist die Konfiguration der Layer-7-Prüfungsrichtlinie auf der privaten DMZ abgeschlossen, damit alle TCP-, UDP- und ICMP-Verbindungen von der Client-Zone zur Server-Zone zugelassen werden. Die Richtlinie wendet keine Problembehebung für untergeordnete Kanäle an, sondern bietet ein Beispiel für eine einfache Richtlinie, um die meisten Anwendungsverbindungen zu berücksichtigen.

Internet-DMZ-Richtlinie konfigurieren

Abbildung 6 zeigt die Konfiguration der Internet-DMZ-Richtlinie.

Abbildung 6: Service-Inspektion von der Internet Zone zur DMZ



Service-Inspektion von der Internet Zone zur DMZ

Diese Richtlinie wendet die Layer-7-Inspektion von der Internetzone auf die DMZ an. Dies ermöglicht Verbindungen von der Internetzone zur DMZ und den Rückverkehr von den DMZ-Hosts zu den Internet-Hosts, die die Verbindung hergestellt haben. Die Internet-DMZ-Richtlinie kombiniert die Layer-7-Inspektion mit Adressgruppen, die von ACLs definiert werden, um den Zugriff auf bestimmte Services auf bestimmten Hosts, Gruppen von Hosts oder Subnetzen zu beschränken. Zu diesem Zweck wird eine Klassenzuordnung geschachtelt, die Dienste in einer anderen Klassenzuordnung angibt, die auf eine ACL verweist, um IP-Adressen anzugeben.

1. Definieren Sie Klassenzuordnungen und ACLs, die den Datenverkehr beschreiben, den Sie zwischen Zonen zulassen möchten. Verwenden Sie dabei die zuvor beschriebenen Richtlinien.Es müssen mehrere Klassenzuordnungen für Services verwendet werden, da für den Zugriff auf zwei verschiedene Server unterschiedliche Zugriffsrichtlinien angewendet werden. Internethosts können DNS- und HTTP-Verbindungen zu 172.16.2.2 und SMTP-Verbindungen zu 172.16.2.3 herstellen. Beachten Sie den Unterschied in den Klassenzuordnungen. Die Klassenzuordnungen, die Dienste angeben, verwenden das Schlüsselwort match-any, um die aufgeführten Dienste zuzulassen. Bei den Klassenzuordnungen, die ACLs mit den Service-Klassenzuordnungen verknüpfen, wird das Schlüsselwort match-all verwendet, um zu erfordern, dass beide Bedingungen in der Klassenzuordnung erfüllt werden müssen, um Datenverkehr zuzulassen:
```
configure terminal
 access-list 110 permit ip any host 172.16.2.2
 access-list 111 permit ip any host 172.16.2.3
 class-map type inspect match-any dns-http-class
  match protocol dns
  match protocol http
 class-map type inspect match-any smtp-class
  match protocol smtp
 class-map type inspect match-all dns-http-acl-class
  match access-group 110
  match class-map dns-http-class
 class-map type inspect match-all smtp-acl-class
  match access-group 111
  match class-map smtp-class
```
2. Konfigurieren Sie Richtlinienzuordnungen, um den Datenverkehr anhand der gerade definierten Klassenzuordnungen zu überprüfen:
```
configure terminal
 policy-map type inspect internet-dmz-policy
```

```
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
```

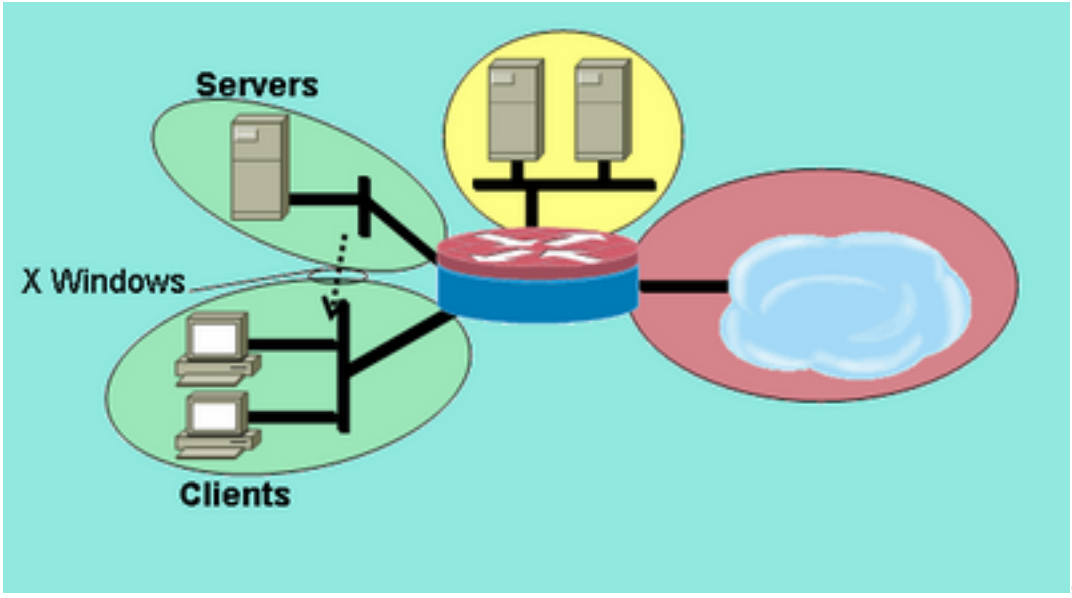
3. Konfigurieren Sie die Internet- und die DMZ-Zone, und weisen Sie den jeweiligen Zonen Router-Schnittstellen zu. Überspringen Sie die DMZ-Konfiguration, wenn Sie sie im vorherigen Abschnitt eingerichtet haben:
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Konfigurieren Sie das Zonenpaar, und wenden Sie die entsprechende Richtlinienzuweisung an.**Anmerkung:** Sie müssen derzeit nur das Internet-DMZ-Zonenpaar konfigurieren, um die Verbindungen zu überprüfen, die von der Internetzone stammen, die zur DMZ führt (siehe nächstes Beispiel):
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
Damit ist die Konfiguration der adressspezifischen Layer-7-Inspektionsrichtlinie für das Internet-DMZ-Zonenpaar abgeschlossen.

Stateful Inspection, transparente Firewall

Server-Clients-Richtlinie konfigurieren

Die folgende Abbildung zeigt die Konfiguration der Server-Client-Richtlinie.

Abbildung 7: Serviceinspektion von Serverzone zu Clientzone



Serviceinspektion von Serverzone zu Clientzone

Die Server-Clients-Richtlinie führt eine Überprüfung mit einem benutzerdefinierten Dienst durch. Die Layer-7-Inspektion wird von der Serverzone auf die Clientzone angewendet. Dadurch können X Windows-Verbindungen zu einem bestimmten Port-Bereich von der Server-Zone zur Client-Zone hergestellt werden, und der zurückfließende Datenverkehr wird zugelassen. X Windows ist

kein natives unterstütztes Protokoll in PAM, daher muss ein benutzerkonfigurierter Dienst in PAM definiert werden, damit die ZFW den entsprechenden Datenverkehr erkennen und überprüfen kann.

Zwei oder mehr Router-Schnittstellen werden in einer IEEE-Bridge-Gruppe konfiguriert, um Integrated Routing and Bridging (IRB) für das Bridging zwischen den Schnittstellen in der Bridge-Gruppe und für die Weiterleitung an andere Subnetze über die Bridge Virtual Interface (BVI) bereitzustellen. Die transparente Firewall-Richtlinie führt eine Firewall-Überprüfung für den Datenverkehr durch, der die Bridge passiert, nicht jedoch für den Datenverkehr, der die Bridge-Gruppe über das BVI verlässt. Die Überprüfungsrichtlinie gilt nur für den Verkehr, der die Brückengruppe passiert. In diesem Szenario wird die Überprüfung daher nur auf Datenverkehr angewendet, der sich zwischen den Client- und Serverzonen bewegt, die innerhalb der privaten Zone geschachtelt sind. Die zwischen der privaten Zone sowie der öffentlichen und der DMZ-Zone angewendete Richtlinie kommt nur zum Tragen, wenn der Datenverkehr die Bridge-Gruppe über das BVI verlässt. Wenn Datenverkehr über die BVI aus den Client- oder Serverzonen austritt, wird die transparente Firewall-Richtlinie nicht aufgerufen.

1. Konfigurieren Sie PAM mit einem benutzerdefinierten Eintrag für X Windows.X Windows-Clients (auf denen Anwendungen gehostet werden) öffnen Verbindungen für die Anzeige von Informationen für Clients (auf denen der Benutzer arbeitet) in einem Bereich, der bei Port 6900 beginnt.Jede zusätzliche Verbindung verwendet aufeinander folgende Ports. Wenn ein Client also 10 verschiedene Sitzungen auf einem Host anzeigt, verwendet der Server die Ports 6900-6909. Wenn Sie den Port-Bereich von 6900 bis 6909 überprüfen, schlagen Verbindungen mit Ports nach 6909 fehl:
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. Lesen Sie die PAM-Dokumente, um zusätzliche PAM-Fragen zu beantworten, oder sehen Sie in der Dokumentation zur detaillierten Protokollprüfung nach, um Informationen zur Interoperabilität zwischen PAM und der Stateful Inspection für die Cisco IOS Firewall zu erhalten.
3. Definieren Sie Klassenzuordnungen, die den Datenverkehr zwischen Zonen beschreiben, den Sie auf der Grundlage der weiter oben beschriebenen Richtlinien zulassen möchten:
```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. Konfigurieren Sie Richtlinienzuordnungen, um den Datenverkehr anhand der gerade definierten Klassenzuordnungen zu überprüfen:
```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```
5. Konfigurieren Sie die Client- und Serverzonen, und weisen Sie den jeweiligen Zonen Router-Schnittstellen zu.Wenn Sie diese Zonen und zugewiesenen Schnittstellen im Abschnitt "Clients-Server-Richtlinienkonfiguration" konfiguriert haben, können Sie mit der Zonenpaar-Definition fortfahren. Der Vollständigkeit halber wird eine Bridging-IRB-Konfiguration bereitgestellt:
```
configure terminal
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
 int vlan 1
 bridge-group 1
```

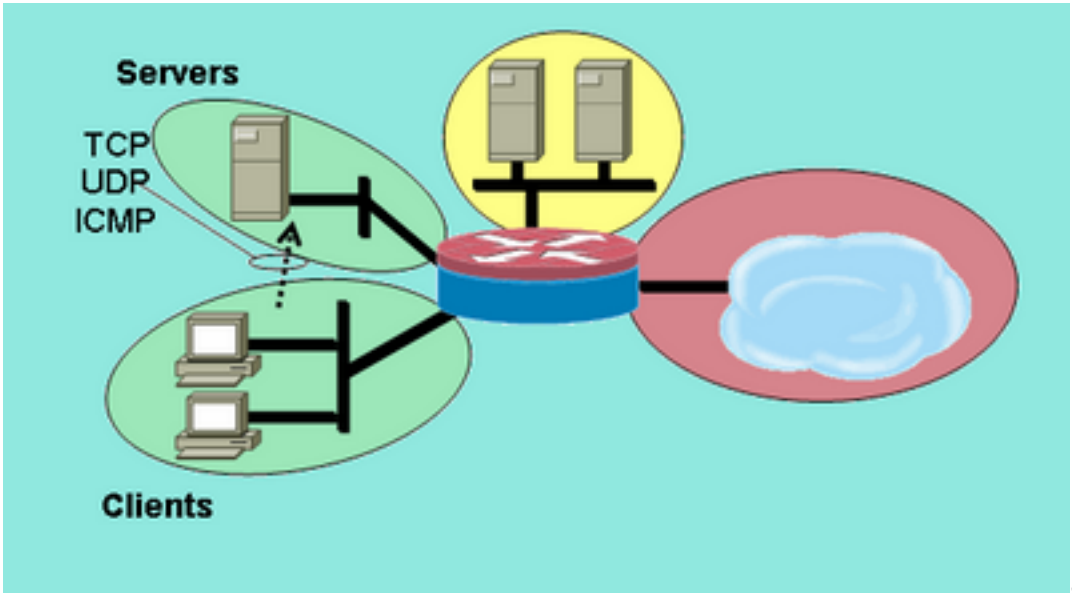
```
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```

6. Konfigurieren Sie das Zonenpaar, und wenden Sie die entsprechende Richtlinienzuweisung an.**Anmerkung:** Sie müssen derzeit nur das Zonenpaar Server-Clients konfigurieren, um die Verbindungen zu überprüfen, die von der Serverzone stammen und zur Clientzone weitergeleitet werden (siehe nächstes Beispiel):
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```
Damit ist die Konfiguration der benutzerdefinierten Prüfungsrichtlinie im Zonenpaar Server-Clients abgeschlossen, sodass X Windows-Verbindungen von der Serverzone zur Clientzone zugelassen werden.

Client-Server-Richtlinie konfigurieren

Abbildung 8 zeigt die Konfiguration der Client-Server-Richtlinie.

Abbildung 8: Serviceinspektion von der Client-Zone zur Server-Zone



Serviceinspektion von der Client-Zone zur Server-Zone

Die Client-Server-Richtlinie ist weniger komplex als die anderen Richtlinien. Die Layer-4-Inspektion wird von der Client-Zone auf die Server-Zone angewendet. Dies ermöglicht Verbindungen von der Client-Zone zur Server-Zone und Rückverkehr. Die Layer-4-Inspektion bietet den Vorteil einer einfachen Firewall-Konfiguration, da nur wenige Regeln erforderlich sind, um den Großteil des Anwendungsdatenverkehrs zu ermöglichen. Die Layer-4-Inspektion bringt jedoch auch zwei wesentliche Nachteile mit sich:

- Anwendungen wie FTP oder Mediendienste handeln häufig einen zusätzlichen untergeordneten Kanal vom Server zum Client aus. Diese Funktionalität wird in der Regel in einem Service-Fix untergebracht, das den Steuerkanal-Dialog überwacht und den untergeordneten Kanal zulässt. Diese Funktion ist bei der Layer-4-Inspektion nicht verfügbar.
- Die Layer-4-Inspektion ermöglicht fast den gesamten Datenverkehr auf Anwendungsebene. Wenn die Netzwerknutzung kontrolliert werden muss, damit nur wenige Anwendungen durch die Firewall zugelassen werden, muss für ausgehenden Datenverkehr eine ACL konfiguriert

werden, um die über die Firewall zulässigen Services zu begrenzen.

Beide Router-Schnittstellen werden in einer IEEE-Bridge-Gruppe konfiguriert, sodass diese Firewall-Richtlinie eine transparente Firewall-Inspektion anwendet. Diese Richtlinie wird auf zwei Schnittstellen in einer IEEE-IP-Bridge-Gruppe angewendet. Die Prüfrichtlinie gilt nur für Datenverkehr, der die Bridge-Gruppe durchquert. Dies erklärt, warum die Client- und Serverzonen innerhalb der privaten Zone geschachtelt sind.

1. Definieren Sie Klassenzuordnungen, die den Datenverkehr zwischen Zonen beschreiben, den Sie auf der Grundlage der weiter oben beschriebenen Richtlinien zulassen möchten:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. Konfigurieren Sie Richtlinienzuordnungen, um den Datenverkehr anhand der gerade definierten Klassenzuordnungen zu überprüfen:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. Konfigurieren Sie die Zonen für Clients und Server, und weisen Sie den jeweiligen Zonen Router-Schnittstellen zu:
```
configure terminal
 zone security clients
 zone security servers
 interface vlan 1
  zone-member security clients
 interface vlan 2
  zone-member security servers
```
4. Konfigurieren Sie das Zonenpaar, und wenden Sie die entsprechende Richtlinienzuweisung an.**Anmerkung:** Sie müssen derzeit nur das Zonenpaar "clients-servers" konfigurieren, um die Verbindungen zu überprüfen, die von der Zone "clients" stammen und zur Zone "servers" weitergeleitet werden (siehe nächstes Beispiel):
```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
Damit ist die Konfiguration der Layer-4-Prüfungsrichtlinie für das Client-Server-Zonenpaar abgeschlossen, sodass alle TCP-, UDP- und ICMP-Verbindungen von der Client-Zone zur Server-Zone zugelassen werden. Die Richtlinie wendet keine Fixups für untergeordnete Kanäle an, sondern bietet ein Beispiel für eine einfache Richtlinie, um die meisten Anwendungsverbindungen zu unterstützen.

Rate-Richtlinie für zonenbasierte Richtlinien-Firewall

Datennetzwerke profitieren häufig von der Möglichkeit, die Übertragungsrate bestimmter Arten von Netzwerkverkehr zu begrenzen und die Auswirkungen von Datenverkehr mit geringerer Priorität auf geschäftskritischen Datenverkehr zu begrenzen. Die Cisco IOS Software bietet diese Funktion mit Traffic Policing, das die nominale Rate und den Burst des Datenverkehrs begrenzt. Die Cisco IOS Software unterstützt die Datenverkehrsüberwachung seit Cisco IOS Version 12.1(5)T.

Die Cisco IOS Software, Version 12.4(9)T, erweitert ZFW um eine Durchsatzratenbegrenzung, wenn Sie die anzuwendende Funktion zur Regelung des Datenverkehrs hinzufügen, der den Definitionen einer bestimmten Klassenzuordnung entspricht, wenn er die Firewall von einer Sicherheitszone zu einer anderen durchquert. Dies bietet den Vorteil, dass ein

Konfigurationspunkt den spezifischen Datenverkehr beschreiben, Firewall-Richtlinien anwenden und die Bandbreitennutzung kontrollieren kann. Die ZFW unterscheidet sich von schnittstellenbasierten Anwendungen dadurch, dass sie nur die Aktionen zur Richtlinienkonformität überträgt und diese bei Richtlinienverletzungen verwirft. ZFW kann keinen Datenverkehr für DSCP markieren.

ZFW kann die Bandbreitennutzung nur in Byte/Sekunde angeben, Pakete/Sekunde und kein Bandbreitenprozentsatz werden angeboten. ZFW kann mit oder ohne schnittstellenbasierter Applikation eingesetzt werden. Wenn daher zusätzliche Funktionen erforderlich sind, können diese über eine Schnittstelle angewendet werden. Wenn eine schnittstellenbasierte Verbindung mit einer Firewall verwendet wird, stellen Sie sicher, dass die Richtlinien nicht in Konflikt miteinander geraten.

ZFW-Richtlinie konfigurieren

Die ZFW-Richtlinienvergabe beschränkt den Datenverkehr in einer Richtlinienzuordnung (Class-Map) auf einen benutzerdefinierten Wert für die Übertragungsrate zwischen 8.000 und 2.000.000 Bits pro Sekunde, wobei ein konfigurierbarer Burst-Wert zwischen 1.000 und 512.000.000 Byte liegt.

Die ZFW-Richtlinienvergabe wird durch eine zusätzliche Konfigurationszeile in der Richtlinienzuweisung konfiguriert, die nach der Richtlinienaktion angewendet wird:

```
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect
  police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

Sitzungssteuerung

Die ZFW-Richtlinie führte außerdem eine Sitzungssteuerung ein, um die Sitzungsanzahl für Datenverkehr in einer anzuwendenden Richtlinienzuordnung zu begrenzen, die einer Klassenzuordnung entspricht. Damit wird die aktuelle Funktion zur Anwendung der DoS-Schutzrichtlinie pro Klassenzuordnung erweitert. Dies ermöglicht eine präzise Kontrolle der Anzahl der anzuwendenden Sitzungen, die mit einer Klassenzuordnung übereinstimmt, die ein Zonenpaar kreuzt. Wenn dieselbe Klassenzuordnung auf mehreren Richtlinienzuordnungen oder Zonenpaaren verwendet wird, können für die verschiedenen Klassenzuordnungsanwendungen unterschiedliche Sitzungslimits angewendet werden.

Die Sitzungssteuerung wird angewendet, wenn eine Parameterzuordnung konfiguriert wurde, die das gewünschte Sitzungsvolumen enthält. Anschließend wird die Parameterzuordnung an die Überprüfungsaktion angefügt, die auf eine Klassenzuordnung unter einer Richtlinienzuordnung angewendet wird:

```
parameter-map type inspect my-parameters
 sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
```

Parameterzuordnungen können nur auf die Aktion "inspect" angewendet werden und sind bei Weiterleitungs- oder Löschaktionen nicht verfügbar.

Die ZFW-Sitzungssteuerungs- und Richtlinienaktivitäten werden mit dem folgenden Befehl angezeigt:

```
show policy-map type inspect zone-pair
```

Anwendungsinspektion

Die Anwendungsinspektion erweitert die Funktionalität von ZFW.
Anwendungsinspektionsrichtlinien werden auf Layer 7 des OSI-Modells angewendet, in dem Benutzeranwendungen Meldungen senden und empfangen, die es ihnen ermöglichen, nützliche Funktionen bereitzustellen. Einige Anwendungen können unerwünschte oder anfällige Funktionen bieten, daher müssen die mit diesen Funktionen verbundenen Meldungen gefiltert werden, um die Aktivitäten für die Anwendungsdienste einzuschränken.

Die Cisco IOS Software ZFW bietet Anwendungsinspektion und -kontrolle für folgende Anwendungsservices:

- HTTP
- SMTP
- POP3
- IMAP
- Sun-RPC
- P2P-Anwendungsdatenverkehr
- IM-Anwendungen

Die Funktionen für Application Inspection and Control (AIC) variieren je nach Service. HTTP Inspection bietet eine präzise Filterung verschiedener Arten von Anwendungsaktivitäten und bietet Funktionen zur Begrenzung der Übertragungsgröße, der Webadressenlänge und der Browseraktivität, um die Einhaltung von Standards für das Verhalten von Anwendungen durchzusetzen und die Arten von Inhalten zu begrenzen, die über den Service übertragen werden. AIC für SMTP kann die Inhaltslänge begrenzen und Protokollkonformität durchsetzen. Die POP3- und IMAP-Prüfung kann sicherstellen, dass Benutzer sichere Authentifizierungsmechanismen verwenden, um eine Beeinträchtigung der Benutzeranmeldeinformationen zu verhindern.

Die Anwendungsinspektion wird als zusätzlicher Satz anwendungsspezifischer Klassenzuordnungen und Richtlinienzuordnungen konfiguriert. Diese werden dann auf die aktuellen Inspektionsklassen- und Richtlinienzuordnungen angewendet, wenn Sie die Anwendungsservicerichtlinie in der Inspektionsrichtlinienzuordnung definieren.

HTTP-Anwendungsinspektion

Die Anwendungsprüfung kann auf den HTTP-Datenverkehr angewendet werden, um die unerwünschte Verwendung des HTTP-Service-Ports für andere Anwendungen wie IM, P2P-Dateifreigabe und Tunneling-Anwendungen zu steuern, die sonst über TCP 80 mit Firewalls verbundene Anwendungen umleiten können.

Konfigurieren Sie eine Klassenzuordnung für die Anwendungsinspektion, um Datenverkehr zu beschreiben, der gegen zulässigen HTTP-Datenverkehr verstößt:

```
! configure the actions that are not permitted
```

```
class-map type inspect http match-any http-aic-cmap
 match request port-misuse any
 match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
 class type insp http http-aic-cmap
  reset
  log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
 match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
 match protocol smtp
 match protocol dns
 match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
 class type inspect http-cmap
  inspect
  service-policy http http-aic-pmap
 class type inspect other-traffic-cmap
  inspect
```

Verbesserte HTTP-Anwendungsinspektion

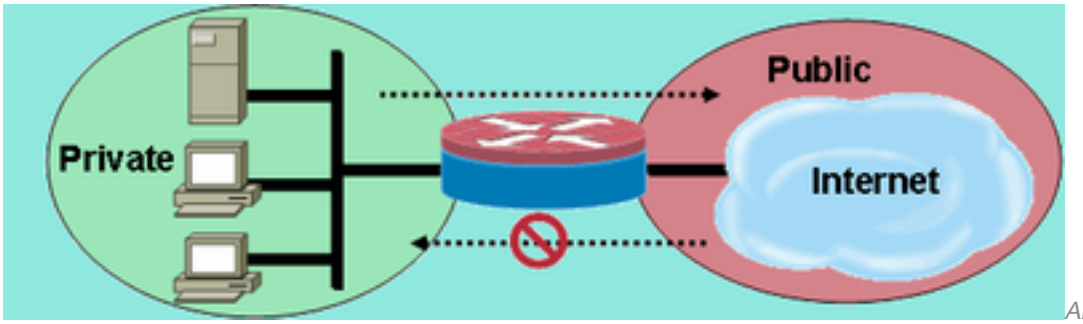
Die Cisco IOS Software, Version 12.4(9)T, enthält Verbesserungen der ZFW-HTTP-Prüfungsfunktionen. Mit Version 12.3(14)T der Cisco IOS Firewall wurde HTTP Application Inspection eingeführt. Die Cisco IOS Software Version 12.4(9)T erweitert die aktuellen Funktionen, wenn Sie Folgendes hinzufügen:

- Möglichkeit zum Zulassen, Ablehnen und Überwachen von Anfragen und Antworten basierend auf Header-Namen und Header-Werten. Dies ist nützlich, um Anfragen und Antworten zu blockieren, die anfällige Header-Felder enthalten.
- Möglichkeit, die Größe verschiedener Elemente im HTTP-Anforderungs- und Antwort-Header zu begrenzen, z. B. maximale URL-Länge, maximale Header-Länge, maximale Header-Zeilenlänge usw. Dies ist nützlich, um Pufferüberläufe zu verhindern.
- Blockieren von Anfragen und Antworten mit mehreren Headern desselben Typs z. B. eine Anfrage mit zwei Content-Length-Headern.
- Möglichkeit, Anfragen und Antworten mit Headern zu blockieren, die nicht ASCII-basiert sind. Dies ist nützlich, um verschiedene Angriffe zu verhindern, die binäre und andere nicht-ASCII-Zeichen verwenden, um Würmer und andere schädliche Inhalte an Webserver zu übermitteln.
- Die Möglichkeit, HTTP-Methoden in benutzerdefinierten Kategorien zu gruppieren, sowie die Flexibilität, jede einzelne Gruppe zu blockieren/zuzulassen/zu überwachen, werden angeboten. Der HTTP-RFC ermöglicht einen eingeschränkten Satz von HTTP-Methoden. Einige der Standardmethoden werden als unsicher betrachtet, da sie zur Ausnutzung von Schwachstellen auf einem Webserver verwendet werden können. Viele der nicht standardmäßigen Methoden weisen eine schlechte Sicherheitsbilanz auf.
- Methode zum Blockieren bestimmter URIs auf der Grundlage eines benutzerdefinierten regulären Ausdrucks. Mit dieser Funktion können Benutzer benutzerdefinierte URIs und Abfragen blockieren.
- Möglichkeit, Header-Typen (insbesondere Server-Header-Typen) mit benutzerdefinierten Zeichenfolgen zu manipulieren. Dies ist nützlich, wenn ein Angreifer Webserver-Antworten analysiert und so viele Informationen wie möglich erhält, und dann einen Angriff startet, der

Schwachstellen in diesem Webserver ausnutzt.
- Möglichkeit, eine HTTP-Verbindung zu blockieren oder eine Warnung auszugeben, wenn ein oder mehrere HTTP-Parameterwerte mit Werten übereinstimmen, die vom Benutzer als regulärer Ausdruck eingegeben wurden. Zu den möglichen HTTP-Wertkontexten gehören Header, Text, Benutzername, Passwort, Benutzer-Agent, Anforderungszeile, Statuszeile und dekodierte CGI-Variablen.

Konfigurationsbeispiele für Verbesserungen bei der HTTP-Anwendungsprüfung setzen ein einfaches Netzwerk voraus (siehe Abbildung 9).

Abbildung 9: Anwendungsinspektion setzt einfaches Netzwerk voraus



Anwendungsinspektion setzt einfaches Netzwerk voraus

Die Firewall gruppiert den Datenverkehr in zwei Klassen:

- HTTP-Datenverkehr
- Alle anderen TCP-, UDP- und ICMP-Zugriffe auf einen Kanal

HTTP wird getrennt, um eine spezifische Überprüfung des Web-Datenverkehrs zu ermöglichen. Auf diese Weise können Sie Richtlinien im ersten Abschnitt dieses Dokuments und HTTP-Anwendungsinspektion im zweiten Abschnitt konfigurieren. Im dritten Abschnitt dieses Dokuments können Sie spezifische Klassenzuordnungen und Richtlinienzuordnungen für P2P- und IM-Datenverkehr konfigurieren. Verbindungen sind von der privaten Zone zur öffentlichen Zone zulässig. Es wird keine Verbindung zwischen der öffentlichen und der privaten Zone bereitgestellt.

In Anhang C finden Sie eine vollständige Konfiguration zur Implementierung der ursprünglichen Richtlinie.

Verbesserte HTTP-Anwendungsinspektion konfigurieren

Die HTTP-Anwendungsinspektion (sowie andere Anwendungsinspektionsrichtlinien) erfordert eine komplexere Konfiguration als die grundlegende Layer-4-Konfiguration. Sie müssen die Layer-7-Datenverkehrsklassifizierung und -richtlinie konfigurieren, um bestimmten Datenverkehr zu erkennen, den Sie steuern möchten, und um die gewünschte Aktion auf gewünschten und unerwünschten Datenverkehr anzuwenden.

Die HTTP-Anwendungsinspektion (ähnlich wie andere Typen der Anwendungsinspektion) kann nur auf den HTTP-Datenverkehr angewendet werden. Daher müssen Sie Layer-7-Klassenzuordnungen und Richtlinienzuordnungen für bestimmten HTTP-Datenverkehr definieren, dann eine Layer-4-Klassenzuordnung speziell für HTTP definieren und die Layer-7-Richtlinie auf die HTTP-Prüfung in einer Layer-4-Richtlinienzuordnung anwenden:

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
```

```
 match  req-resp protocol-violation
 match  request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
 class type inspect http http-l7-cmap
  reset
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all http-l4-cmap
 match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap
```

Alle diese HTTP-Anwendungsinspektions-Datenverkehrsmerkmale werden in einer Layer-7-Klassenzuordnung definiert:

- Der Header Inspection-Befehl bietet die Möglichkeit, Anforderungen oder Antworten zuzulassen/abzulehnen/zu überwachen, deren Header mit dem konfigurierten regulären Ausdruck übereinstimmt. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:
  `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  Befehlsverwendung:

```
match {request|response|req-resp} header regex <parameter-map-name>
```

Anwendungsbeispiel

- Konfigurieren Sie eine http appfw-Richtlinie, um eine Anfrage oder Antwort zu blockieren, deren Header keine ASCII-Zeichen enthält.

```
parameter-map type regex non_ascii_regex
   pattern “[^\x00-\x80]”
class-map type inspect http non_ascii_cm
   match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
   class type inspect http non_ascii_cm
      reset
```

Header-Längenüberprüfung - Mit diesem Befehl wird die Länge eines Anforderungs- oder Antwortheaders überprüft und eine Aktion angewendet, wenn die Länge den konfigurierten Grenzwert überschreitet. Aktion ist zulässig oder wird zurückgesetzt. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-4- HTTP_HEADER_LENGTH
```

Befehlsverwendung:

```
match {request|response|req-resp} header length gt <bytes>
```

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um Anforderungen und Antworten zu blockieren, deren Header-Länge mehr als 4096 Byte beträgt.

```
class-map type inspect http hdr_len_cm
   match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
   class type inspect http hdr_len_cm
      reset
```

Header Count Inspection - Mit diesem Befehl wird die Anzahl der Header-Zeilen (Felder) in einer Anfrage/Antwort überprüft und eine Aktion angewendet, wenn die Anzahl den konfigurierten Grenzwert überschreitet. Aktion ist zulässig oder wird zurückgesetzt. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6- HTTP_HEADER_COUNT
```

Befehlsverwendung:

```
match {request|response|req-resp} header count gt <number>
```

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um eine Anforderung mit mehr als 16 Headerfeldern zu blockieren.

```
class-map type inspect http hdr_cnt_cm
   match request header count gt 16

policy-map type inspect http hdr_cnt_pm
   class type inspect http hdr_cnt_cm
      reset
```

Header Field Inspection - Dieser Befehl ermöglicht das Zulassen/Verweigern/Überwachen von Anfragen/Antworten, die ein bestimmtes HTTP-Header-Feld und einen bestimmten HTTP-Header-Wert enthalten. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

Befehlsverwendung:

```
match {request|response|req-resp} header <header-name>
```

Anwendungsbeispiel

Konfigurieren Sie eine HTTP-Anwendungsinspektionsrichtlinie, um Spyware/Adware zu blockieren:

```
parameter-map type regex ref_regex
   pattern “\.delfinproject\.com”
```

```
   pattern “\.looksmart\.com”

parameter-map type regex host_regex
   pattern “secure\.keenvalue\.com”
   pattern “\.looksmart\.com”

parameter-map type regex usragnt_regex
   pattern “Peer Points Manager”

class-map type inspect http spy_adwr_cm
   match request header refer regex ref_regex
   match request header host regex host_regex
   match request header user-agent regex usragnt_regex

policy-map type inspect http spy_adwr_pm
   class type inspect http spy_adwr_cm
      reset
```

Header-Feldlängenprüfung - Dieser Befehl bietet die Möglichkeit, die Länge einer Header-Feldzeile zu begrenzen. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

Befehlsverwendung:

```
match {request|response|req-resp} header <header-name> length gt <bytes>
```

Anwendungsbeispiel

Konfigurieren Sie eine HTTP-Appfw-Richtlinie, um eine Anforderung zu blockieren, deren Cookie- und Benutzer-Agent-Feldlänge 256 bzw. 128 überschreitet.

```
class-map type inspect http hdrline_len_cm
   match request header cookie length gt 256
   match request header user-agnet length gt 128

policy-map type inspect http hdrline_len_pm
   class type inspect http hdrline_len_cm
      reset
```

Überprüfung der Wiederholung von Headerfeldern - Mit diesem Befehl wird geprüft, ob eine Anforderung oder Antwort über wiederholte Headerfelder verfügt. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Wenn die Protokollaktion aktiviert ist, wird eine Syslog-Meldung ausgegeben:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

Befehlsverwendung:

```
match {request|response|req-resp} header <header-name>
```

Anwendungsbeispiel

Konfigurieren Sie eine HTTP-Appfw-Richtlinie, um eine Anforderung oder Antwort mit mehreren Headerzeilen in Inhaltslänge zu blockieren. Dies ist eine der nützlichsten Funktionen, um

Sitzungsschmuggel zu verhindern.

```
class-map type inspect http multi_occrns_cm
   match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
   class type inspect http multi_occrns_cm
      reset
```

- Method Inspection - Die HTTP-RFC ermöglicht einen eingeschränkten Satz von HTTP-Methoden. Allerdings gelten auch einige der Standardmethoden als unsicher, da einige Methoden verwendet werden können, um Schwachstellen auf einem Webserver auszunutzen. Viele der nicht standardmäßigen Methoden werden häufig für schädliche Aktivitäten verwendet. Dies erfordert eine Notwendigkeit, die Methoden in verschiedene Kategorien zu gruppieren und den Benutzer die Aktion für jede Kategorie wählen zu lassen. Dieser Befehl bietet dem Benutzer eine flexible Möglichkeit, die Methoden in verschiedene Kategorien wie sichere Methoden, unsichere Methoden, webdav-Methoden, RFC-Methoden und erweiterte Methoden zu gruppieren. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6-HTTP_METHOD
```

Befehlsverwendung:

```
match request method <method>
```

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, die die HTTP-Methoden in drei Kategorien gruppiert: sicher, unsicher und webdav. Diese werden in der nächsten Tabelle aufgeführt. Konfigurieren Sie Aktionen wie:

- Alle sicheren Methoden sind ohne Protokoll zulässig.
- Alle unsicheren Methoden sind mit log erlaubt
- Alle webdav-Methoden werden mit log blockiert.

Safe	Unsicher	WebDAV
GET, HEAD, OPTION	POST, PUT, CONNECT, TRACE	KOPIEREN, LÖSCHEN, BEWEGEN

```
http policy:

class-map type inspect http safe_methods_cm
   match request method get
   match request method head
   match request method option

class-map type inspect http unsafe_methods_cm
   match request method post
   match request method put
   match request method connect
   match request method trace

class-map type inspect http webdav_methods_cm
   match request method bcopy
   match request method bdelete
```

```
   match request method bmove

policy-map type inspect http methods_pm
   class type inspect http safe_methods_cm
      allow
   class type inspect http unsafe_methods_cm
      allow log
      class type inspect http webdav_methods_cm
      reset log
```

URI-Überprüfung - Dieser Befehl ermöglicht das Zulassen/Verweigern/Überwachen von Anforderungen, deren URI mit der konfigurierten regulären Überprüfung übereinstimmt. Dadurch kann der Benutzer benutzerdefinierte URLs und Abfragen blockieren. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

Befehlsverwendung:

```
match request uri regex <parameter-map-name>
```

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um eine Anforderung zu blockieren, deren URI mit einem der folgenden regulären Ausdrücke übereinstimmt:

- .*cmd.exe
- * Geschlecht
- * Glücksspiel

```
parameter-map type regex uri_regex_cm
   pattern ".*cmd.exe"
   pattern ".*sex"
   pattern ".*gambling"

class-map type inspect http uri_check_cm
   match request uri regex uri_regex_cm

policy-map type inspect http uri_check_pm
   class type inspect http uri_check_cm
      reset
```

- URI-Längenüberprüfung - Dieser Befehl überprüft die Länge des URIs, der in einer Anforderung gesendet wird, und wendet die konfigurierte Aktion an, wenn die Länge den konfigurierten Grenzwert überschreitet. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

  ```
  APPFW-6- HTTP_URI_LENGTH
  ```

  Befehlsverwendung:

  ```
  match request uri length gt <bytes>
  ```

  Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um einen Alarm auszulösen, wenn die URI-Länge einer Anforderung 3076 Byte überschreitet.

```
class-map type inspect http uri_len_cm
   match request uri length gt 3076

policy-map type inspect http uri_len_pm
   class type inspect http uri_len_cm
      log
```

Argumentüberprüfung - Dieser Befehl ermöglicht das Zulassen, Verweigern oder Überwachen von Anfragen, deren Argumente (Parameter) mit konfigurierten regulären Überprüfungen übereinstimmen. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

Befehlsverwendung:

```
match request arg regex <parameter-map-name>
```

Konfigurieren Sie eine http appfw-Richtlinie, um eine Anforderung zu blockieren, deren Argumente mit einem der folgenden regulären Ausdrücke übereinstimmen:

- .*gezählt
- * Angriff

```
parameter-map type regex arg_regex_cm
   pattern “.*codered”
   pattern “.*attack”

class-map type inspect http arg_check_cm
   match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
   class type inspect http arg_check_cm
      reset
```

- Prüfung der Argumentlänge - Dieser Befehl überprüft die Länge der Argumente, die in einer Anforderung gesendet werden, und wendet die konfigurierte Aktion an, wenn die Länge den konfigurierten Grenzwert überschreitet. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:
  ```
  APPFW-6- HTTP_ARG_LENGTH
  ```
  Befehlsverwendung:
  ```
  match request arg length gt <bytes>
  ```
  Anwendungsbeispiel

Konfigurieren Sie eine HTTP-Appfw-Richtlinie, um einen Alarm auszulösen, wenn die Argumentlänge einer Anforderung 512 Byte überschreitet.

```
class-map type inspect http arg_len_cm
   match request arg length gt 512

policy-map type inspect http arg_len_pm
   class type inspect http arg_len_cm
      log
```

- Body Inspection - Mit dieser CLI kann der Benutzer eine Liste regulärer Ausdrücke angeben,

die dem Text der Anforderung oder Antwort zugeordnet werden sollen. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

`APPFW-6- HTTP_BODY_REGEX_MATCHED`

Befehlsverwendung:

`match {request|response|reg-resp} body regex <parameter-map-name>`

Anwendungsbeispiel

Konfigurieren Sie eine http-App, um eine Antwort zu blockieren, deren Text das Muster `.*[Aa][Tt][Tt][Tt][Aa][Cc][Kk]` enthält.

```
parameter-map type regex body_regex
   pattern “.*[Aa][Tt][Tt][Aa][Cc][Kk]”

class-map type inspect http body_match_cm
   match response body regex body_regex

policy-map type inspect http body_match_pm
   class type inspect http body_match_cm
      reset
```

Prüfung der Länge des Hauptteils (des Inhalts) - Mit diesem Befehl wird die Größe der Nachricht überprüft, die über eine Anfrage oder Antwort gesendet wird. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

`APPFW-4- HTTP_CONTENT_LENGTH`

Befehlsverwendung:

`match {request|response|req-resp} body length lt <bytes> gt <bytes>`

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um eine http-Sitzung zu blockieren, die mehr als 10.000 Byte an Nachrichten in einer Anforderung oder Antwort enthält.

```
class-map type inspect http cont_len_cm
   match req-resp header content-length gt 10240

policy-map type inspect http cont_len_pm
   class type inspect http cont_len_cm
      reset
```

Statuszeilenprüfung - Mit diesem Befehl kann der Benutzer eine Liste regulärer Ausdrücke angeben, die mit der Statuszeile einer Antwort abgeglichen werden sollen. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:

`APPFW-6-HTTP_STLINE_REGEX_MATCHED`

Befehlsverwendung:

```
match response status-line regex <class-map-name>
```

Anwendungsbeispiel

Konfigurieren Sie einen HTTP-Appfw, um einen Alarm zu protokollieren, wenn versucht wird, auf eine verbotene Seite zuzugreifen. Eine verbotene Seite enthält normalerweise einen 403-Statuscode, und die Statuszeile sieht aus wie `HTTP/1.0 403 page forbidden\r\n`.

```
parameter-map type regex status_line_regex
   pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403”

class-map type inspect http status_line_cm
   match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
   class type inspect http status_line_cm
      log
```

- Inhaltstypüberprüfung - Mit diesem Befehl wird überprüft, ob der Inhaltstyp des Nachrichtenkopfs in der Liste der unterstützten Inhaltstypen enthalten ist. Außerdem wird überprüft, ob der Inhaltstyp des Headers mit dem Inhalt der Nachrichtendaten oder des Entitätstextteils übereinstimmt. Wenn das Schlüsselwort nicht übereinstimmt, überprüft der Befehl den Inhaltstyp der Antwortnachricht anhand des akzeptierten Feldwerts der Anforderungsnachricht. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Durch Hinzufügen der Protokollaktion wird die entsprechende Syslog-Meldung ausgegeben:
  ```
  APPFW-4- HTTP_CONT_TYPE_VIOLATION
  APPFW-4- HTTP_CONT_TYPE_MISMATCH
  APPFW-4- HTTP_CONT_TYPE_UNKNOWN
  ```
  Befehlsverwendung:
  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```
  AnwendungsbeispielKonfigurieren Sie eine http appfw-Richtlinie, um eine http-Sitzung zu blockieren, die Anforderungen und Antworten mit unbekanntem Inhaltstyp enthält.
  ```
  class-map type inspect http cont_type_cm
     match req-resp header content-type unknown

  policy-map type inspect http cont_type_pm
     class type inspect http cont_type_cm
        reset
  ```

Prüfung auf Port-Missbrauch - Dieser Befehl verhindert, dass der HTTP-Port (80) für andere Anwendungen wie IM, P2P, Tunneling usw. missbraucht wird. Die Aktion "Zulassen" oder "Zurücksetzen" kann auf eine Anforderung oder Antwort angewendet werden, die den Klassenzuordnungskriterien entspricht. Durch Hinzufügen der Protokollaktion wird die entsprechende Syslog-Meldung ausgegeben:

```
APPFW-4- HTTP_PORT_MISUSE_TYPE_IM
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL
```

Befehlsverwendung:

```
match request port-misuse {im|p2p|tunneling|any}
```

Anwendungsbeispiel

Konfigurieren Sie eine http appfw-Richtlinie, um eine HTTP-Sitzung zu blockieren, die für eine IM-Anwendung missbraucht wird.

```
class-map type inspect http port_misuse_cm
   match request port-misuse im

policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
```

- Strict-HTTP Inspection: Dieser Befehl ermöglicht die strenge Prüfung der Protokollkonformität in Bezug auf HTTP-Anfragen und -Antworten. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:
  `APPFW-4- HTTP_PROTOCOL_VIOLATION`
  Befehlsverwendung:
  `match req-resp protocol-violation`
  AnwendungsbeispielKonfigurieren Sie eine http appfw-Richtlinie, um Anforderungen oder Antworten zu blockieren, die gegen RFC 2616 verstoßen:
  ```
  class-map type inspect http proto-viol_cm
     match req-resp protocol-violation

  policy-map type inspect http proto-viol_pm
     class type inspect http proto-viol_cm
        reset
  ```
- Transfer- Encoding Inspection — Dieser Befehl ermöglicht das Zulassen, Verweigern oder Überwachen von Anfragen/Antworten, deren Codierungstyp mit dem konfigurierten Typ übereinstimmt. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:
  `APPFW-6- HTTP_TRANSFER_ENCODING`
  Befehlsverwendung:
  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```
  AnwendungsbeispielKonfigurieren Sie eine HTTP-AppFw-Richtlinie, um eine Anforderung oder Antwort mit Codierung des Komprimierungstyps zu blockieren.
  ```
  class-map type inspect http trans_encoding_cm
     match req-resp header transfer-encoding type compress

  policy-map type inspect http trans_encoding_pm
     class type inspect http trans_encoding_cm
        reset
  ```
- Java Applet Inspection - Dieser Befehl überprüft, ob eine Antwort über ein Java Applet verfügt, und wendet die konfigurierte Aktion bei Erkennung eines Applet an. Die Aktion Zulassen oder Zurücksetzen kann auf eine Anforderung oder Antwort angewendet werden, die den Kriterien für die Klassenzuordnung entspricht. Das Hinzufügen der Protokollaktion verursacht eine Syslog-Meldung:
  `APPFW-4- HTTP_JAVA_APPLET`
  Befehlsverwendung:
  `match response body java-applet`
  AnwendungsbeispielKonfigurieren Sie eine http appfw-Richtlinie, um Java-Applets zu blockieren.
  ```
  class-map type inspect http java_applet_cm
     match response body java-applet
  ```

```
policy-map type inspect http java_applet_pm
   class type inspect http java_applet_cm
      reset
```

ZFW-Unterstützung für Instant Messaging und Peer-to-Peer-Anwendungskontrolle

Mit der Cisco IOS Software-Version 12.4(9)T wurde die ZFW-Unterstützung für IM- und P2P-Anwendungen eingeführt.

Die Cisco IOS Software bietet erstmals Unterstützung für die IM-Anwendungssteuerung in Version 12.4(4)T der Cisco IOS Software. Die erste Version von ZFW unterstützte keine IM-Anwendung in der ZFW-Schnittstelle. Wenn eine IM-Anwendungssteuerung gewünscht wurde, konnten die Benutzer nicht zur ZFW-Konfigurationsschnittstelle migrieren. Cisco IOS Software Release 12.4(9)T bietet ZFW-Unterstützung für IM Inspection, die Yahoo! Messenger (YM), MSN Messenger (MSN) und AOL Instant Messenger (AIM). Cisco IOS Software Release 12.4(9)T ist die erste Version der Cisco IOS Software, die native Unterstützung der Cisco IOS Firewall für P2P-Dateifreigabeanwendungen bietet.

Sowohl IM als auch P2P Inspection bieten Layer-4- und Layer-7-Richtlinien für den Anwendungsdatenverkehr. Das bedeutet, dass ZFW grundlegende Stateful-Inspection-Funktionen zum Zulassen oder Verweigern des Datenverkehrs bereitstellen kann, sowie eine granulare Layer-7-Kontrolle bestimmter Aktivitäten in den verschiedenen Protokollen, sodass bestimmte Anwendungsaktivitäten zugelassen werden, während andere abgelehnt werden.

P2P-Anwendungsinspektion und -kontrolle

In SDM 2.2 wurde die P2P-Anwendungskontrolle im Abschnitt zur Firewall-Konfiguration eingeführt. SDM wandte eine Network-Based Application Recognition (NBAR)- und eine QoS-Richtlinie an, um P2P-Anwendungsaktivitäten zu erkennen und auf eine Leitungsrate von Null zu regeln und den gesamten P2P-Datenverkehr zu blockieren. Dies warf das Problem auf, dass CLI-Benutzer, die P2P-Unterstützung in der CLI der Cisco IOS Firewall erwarteten, die P2P-Blockierung in der CLI nur konfigurieren konnten, wenn sie die erforderliche NBAR/QoS-Konfiguration kannten. Mit Version 12.4(9)T der Cisco IOS Software wird die native P2P-Kontrolle in der ZFW-CLI eingeführt, um NBAR zur Erkennung von P2P-Anwendungsaktivitäten zu nutzen. Diese Softwareversion unterstützt mehrere P2P-Anwendungsprotokolle:

- BitTorrent
- eDonkey
- FastTrack
- Gnutella
- KaZaA/KaZaA2
- WinMX

P2P-Anwendungen sind aufgrund des "Port-Hopping"-Verhaltens und anderer Tricks zur Vermeidung von Erkennungen sowie aufgrund häufiger Änderungen und Updates von P2P-Anwendungen, die das Verhalten der Protokolle ändern, besonders schwer zu erkennen. Die ZFW kombiniert die native Stateful Inspection der Firewall mit den Erkennungsfunktionen für den Datenverkehr der NBAR, um eine P2P-Anwendungskontrolle in der CPL-Konfigurationsschnittstelle der ZFW zu ermöglichen. NBAR bietet zwei hervorragende Vorteile:

- Optionale heuristische Anwendungserkennung zur Erkennung von Anwendungen trotz

komplexem, schwer erkennbarem Verhalten
- Erweiterbare Infrastruktur mit Aktualisierungsmechanismus für aktuelle Protokoll-Updates und -Änderungen

Konfigurieren der P2P-Inspektion

Wie bereits erwähnt, bietet die P2P-Inspektion und -Kontrolle sowohl Layer 4 Stateful Inspection als auch Layer 7 Application Control. Die Layer-4-Inspektion wird ähnlich wie andere Anwendungsservices konfiguriert, wenn die Inspektion der nativen Anwendungsservice-Ports ausreichend ist:

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

Beachten Sie die zusätzliche Signaturoption im Übereinstimmungsprotokoll [Dienstname]. Wenn die Signaturoption am Ende der Übereinstimmungsprotokollanweisung hinzugefügt wird, wird die NBAR-Heuristik auf den Datenverkehr angewendet, um nach Auflistungen im Datenverkehr zu suchen, die bestimmte P2P-Anwendungsaktivitäten angeben. Dazu gehören Port-Hopping und andere Änderungen im Anwendungsverhalten, um eine Erkennung des Datenverkehrs zu vermeiden. Diese Prüfung des Datenverkehrs erfolgt auf Kosten einer höheren CPU-Auslastung und eines geringeren Netzwerkdurchsatzes. Wenn die Signaturoption nicht angewendet wird, wird die NBAR-basierte heuristische Analyse nicht angewendet, um das Port-Hopping-Verhalten zu erkennen, und die CPU-Nutzung wird nicht im gleichen Ausmaß beeinträchtigt.

Die native Service-Inspektion hat den Nachteil, dass sie die Kontrolle über P2P-Anwendungen nicht behalten kann, wenn die Anwendung auf einen nicht standardmäßigen Quell- und Zielport "hops" oder wenn die Anwendung aktualisiert wird, um ihre Aktion für eine nicht erkannte Portnummer zu starten:

Anwendung	Native Ports (gemäß 12.4(15)T PAM-Liste)
Bittorrent	TCP 6881-6889
entschlüsseln	TCP 4662
Schnellspur	TCP 1214
Gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
Kazaa2	Abhängig von PAM
Winmx	TCP 6699

Wenn Sie P2P-Datenverkehr zulassen (prüfen) möchten, müssen Sie eine zusätzliche Konfiguration bereitstellen. Einige Anwendungen können mehrere P2P-Netzwerke verwenden oder bestimmte Verhaltensweisen implementieren, die Sie in Ihrer Firewall-Konfiguration berücksichtigen müssen, damit die Anwendung funktioniert:

- BitTorrent-Clients kommunizieren in der Regel mit "Trackern" (Peer-Directory-Server) über HTTP, das auf einigen nicht standardmäßigen Ports ausgeführt wird. Dies ist normalerweise TCP 6969, aber Sie müssen den torrent-spezifischen Tracker-Port überprüfen. Wenn Sie BitTorrent zulassen möchten, ist die beste Methode, den zusätzlichen Port aufzunehmen, HTTP als eines der Übereinstimmungsprotokolle zu konfigurieren und TCP 6969 mit dem Befehl ip port-map zu HTTP hinzuzufügen:

```
ip port-map http port tcp 6969
```

Sie müssen HTTP und Bittorrent als die in der Klassenzuordnung angewendeten Übereinstimmungskriterien definieren.

- eDonkey scheint Verbindungen zu initiieren, die als eDonkey und Gnutella erkannt werden.
- Die KaZaA-Inspektion ist vollständig von der Erkennung von NBAR-Signaturen abhängig.

Die Layer-7-Inspektion (für Anwendungen) erweitert die Layer-4-Inspektion mit der Möglichkeit, servicespezifische Aktionen zu erkennen und anzuwenden, z. B. um Funktionen für die Dateisuche, Dateiübertragung und Textchat selektiv zu blockieren oder zuzulassen. Die servicespezifischen Funktionen variieren je nach Service.

Die P2P-Anwendungsinspektion ähnelt der HTTP-Anwendungsinspektion:

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

P2P Application Inspection bietet anwendungsspezifische Funktionen für einen Teil der Anwendungen, die von Layer-4-Inspektion unterstützt werden:

- entschlüsseln
- Schnellspur
- Gnutella
- Kazaa2

Jede dieser Anwendungen bietet Optionen für variable anwendungsspezifische Anpassungskriterien:

entschlüsseln

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap
router(config-cmap)#match ?
  file-transfer     Match file transfer stream
  flow              Flow based QoS parameters
  search-file-name  Match file name
  text-chat         Match text-chat
```

Schnellspur

```
router(config)#class-map type inspect fasttrack match-any ftrak-l7-cmap
router(config-cmap)#match ?
  file-transfer  File transfer stream
  flow           Flow based QoS parameters
```

Gnutella

```
router(config)#class-map type inspect gnutella match-any gtella-l7-cmap
router(config-cmap)#
```

Kazaa2

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-l7-cmap
router(config-cmap)#match ?
  file-transfer  Match file transfer stream
  flow           Flow based QoS parameters
```

Neue P2P-Protokolldefinitionen oder Aktualisierungen aktueller P2P-Protokolle können mit der dynamischen PDLM-Aktualisierungsfunktion von NBAR geladen werden. Dies ist der Konfigurationsbefehl zum Laden der neuen PDLM:

```
ip nbar pdlm <file-location>
```

Das neue Protokoll ist in Übereinstimmungsprotokollbefehlen für die Klassentypüberprüfung verfügbar. Verfügt das neue P2P-Protokoll über Dienste (Unterprotokolle), stehen die neuen Klassenzuordnungstypen für die Layer-7-Prüfung sowie die Übereinstimmungskriterien für Layer 7 zur Verfügung.

IM-Anwendungsinspektion und -kontrolle

Cisco IOS Software, Version 12.4(4)T, führt IM Application Inspection and Control ein. Die IM-Unterstützung wurde mit ZFW in 12.4(6)T nicht eingeführt, sodass die Benutzer die IM-Kontrolle und ZFW nicht in derselben Firewall-Richtlinie anwenden konnten, da ZFW und ältere Firewall-Funktionen nicht auf einer bestimmten Schnittstelle gleichzeitig vorhanden sein können.

Cisco IOS Software, Version 12.4(9)T, unterstützt Stateful Inspection und Anwendungskontrolle für die folgenden IM-Services:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger

Die IM-Prüfung weicht von den meisten Services leicht ab, da die IM-Prüfung den Zugriff auf eine bestimmte Gruppe von Hosts für jeden bestimmten Service steuert. IM-Dienste basieren im Allgemeinen auf einer relativ permanenten Gruppe von Verzeichnisservern, die von Clients kontaktiert werden können müssen, um auf den IM-Dienst zuzugreifen. IM-Anwendungen lassen sich in der Regel nur schwer vom Protokoll- oder Servicepunkt aus steuern. Die effektivste Möglichkeit, diese Anwendungen zu steuern, besteht darin, den Zugriff auf die festen IM-Server zu beschränken.

IM-Inspektion konfigurieren

IM-Inspektion und -Kontrolle bietet Stateful Inspection für Layer 4

und Layer 7-Anwendungskontrolle.

Die Layer-4-Inspektion wird ähnlich wie andere Anwendungsservices konfiguriert:

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  [drop | inspect | pass
```

IM-Anwendungen können ihre Server über mehrere Ports kontaktieren, um ihre Funktionalität aufrechtzuerhalten. Um einen bestimmten IM-Dienst mit der Aktion "inspect" zuzulassen, ist keine Serverliste erforderlich, um den zulässigen Zugriff auf die Server des IM-Dienstes zu definieren. Wenn Sie jedoch eine Klassenzuordnung konfigurieren, die einen bestimmten IM-Dienst angibt, z. B. AOL Instant Messenger, und die Ablagerungsaktion in der zugeordneten Richtlinienzuordnung anwenden, kann der IM-Client versuchen, einen anderen Port zu finden, an dem die Verbindung zum Internet zulässig ist. Wenn Sie die Konnektivität zu einem bestimmten Dienst nicht zulassen oder die IM-Dienst-Funktionalität auf den Text-Chat beschränken möchten, müssen Sie eine Serverliste definieren, damit der ZFW den mit der IM-Anwendung verknüpften Datenverkehr identifizieren kann:

```
!configure the server-list parameter-map:
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```

Die Liste der IM-Server von Yahoo ist beispielsweise wie folgt definiert:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 10.0.77.88
  server ip range 172.16.0.77 172.16.0.99
```

Sie müssen die Serverliste auf die Protokolldefinition anwenden:

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```

Sie müssen die Befehle ip domain lookup und ip name-server ip.ad.re.ss konfigurieren, um die Namensauflösung zu aktivieren.

IM-Servernamen sind ziemlich dynamisch. Sie müssen in regelmäßigen Abständen überprüfen, ob die von Ihnen konfigurierten IM-Serverlisten vollständig und korrekt sind.

Die Layer-7-Inspektion (für Anwendungen) erweitert die Layer-4-Inspektion mit der Möglichkeit, servicespezifische Aktionen zu erkennen und anzuwenden, z. B. um Textchatfunktionen selektiv zu blockieren oder zuzulassen, und verweigert andere Servicefunktionen.

IM Application Inspection bietet derzeit die Möglichkeit, zwischen Text-Chat-Aktivitäten und allen anderen Anwendungsdiensten zu unterscheiden. Konfigurieren Sie eine Layer-7-Richtlinie, um die IM-Aktivität auf Text-Chats zu beschränken:

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat

class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-text-cmap
    reset
    [log]
```

Wenden Sie die Layer-7-Richtlinie auf Yahoo! Vorher konfigurierte Messenger-Richtlinie:

```
class-map type inspect match-any my-im-class
match protocol ymsgr
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  inspect
  service-policy im ymsgr-l7-pmap
```

URL-Filter

ZFW bietet URL-Filterfunktionen, um den Zugriff auf Webinhalte auf den Zugriff zu beschränken, der durch eine auf dem Router definierte Weiß- oder Blacklist festgelegt wird, oder indem Domänennamen an einen URL-Filterserver weitergeleitet werden, um den Zugriff auf bestimmte Domänen zu überprüfen. Die ZFW-URL-Filterung in den Cisco IOS Software-Versionen 12.4(6)T bis 12.4(15)T wird ähnlich wie die Anwendungsinspektion als zusätzliche Richtlinienaktion angewendet.

Für die serverbasierte URL-Filterung müssen Sie eine Parameterzuordnung definieren, die die urlfilter-Serverkonfiguration beschreibt:

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```

Wenn statische weiße oder schwarze Listen bevorzugt werden, können Sie eine Liste von Domänen oder Subdomänen definieren, die ausdrücklich zugelassen oder abgelehnt werden, während die umgekehrte Aktion auf Datenverkehr angewendet wird, der nicht mit der Liste übereinstimmt:

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```

Wenn in den Definitionen der exklusiven Domäne eine schwarze Liste von URLs mit deny-Optionen definiert wird, sind alle anderen Domänen zulässig. Wenn "Zulassen"-Definitionen definiert sind, müssen alle zulässigen Domänen explizit angegeben werden, ähnlich wie bei IP-Zugriffskontrolllisten.

Richten Sie eine Klassenzuordnung ein, die dem HTTP-Datenverkehr entspricht:

```
class-map type inspect match-any http-cmap
 match protocol http
```

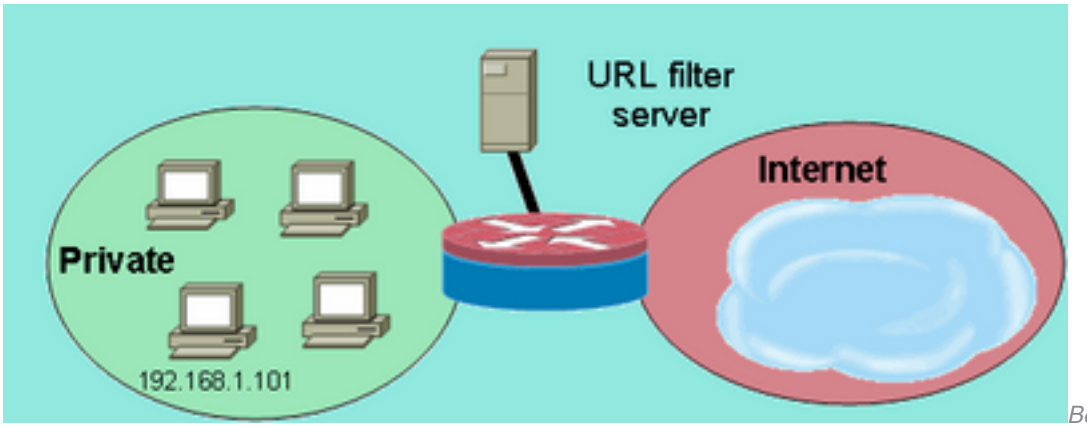
Definieren Sie eine Richtlinienzuordnung, die Ihre Klassenzuordnung mit den Aktionen inspect und urlfilter verknüpft:

```
policy-map type inspect http-filter-pmap
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

Dadurch wird die Mindestanforderung für die Kommunikation mit einem URL-Filterserver konfiguriert. Es stehen mehrere Optionen zur Verfügung, um ein zusätzliches URL-Filterverhalten festzulegen.

Einige Netzwerkbereitstellungen möchten URL-Filterung für einige Hosts oder Subnetze anwenden und die URL-Filterung für andere Hosts umgehen. Beispiel: In Abbildung 9 muss der HTTP-Datenverkehr aller Hosts in der privaten Zone von einem URL-Filterserver überprüft werden, mit Ausnahme des spezifischen Hosts 192.168.1.101.

Abbildung 10: Beispieltopologie für URL-Filterung



Beispieltopologie für URL-Filterung

Dies ist möglich, wenn Sie zwei verschiedene Klassenzuordnungen definieren:

- Eine Klassenzuordnung, die nur für den HTTP-Datenverkehr der größeren Gruppe von Hosts, die URL-Filterung erhalten, übereinstimmt.
- Eine Klassenzuordnung für die kleinere Gruppe von Hosts, die keine URL-Filterung erhalten. Die zweite Klassenzuordnung vergleicht HTTP-Datenverkehr sowie eine Liste von Hosts, die von der URL-Filterrichtlinie ausgenommen sind.

Beide Klassenzuordnungen werden in einer Richtlinienzuordnung konfiguriert, aber nur eine erhält die urlfilter-Aktion:

```
class-map type inspect match-any http-cmap
 match protocol http
class-map type inspect match-all http-no-urlf-cmap
 match protocol http
 match access-group 101
!
policy-map type inspect http-filter-pmap
 class type inspect http-no-urlf-cmap
  inspect
 class type inspect http-cmap
```

```
  inspect
  urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

Zugriffskontrolle für den Router

Die meisten Netzwerksicherheitstechniker fühlen sich unwohl, wenn sie die Verwaltungsschnittstellen des Routers (z. B. SSH, Telnet, HTTP, HTTPS, SNMP usw.) dem öffentlichen Internet zugänglich machen. Unter bestimmten Umständen muss auch der LAN-Zugriff auf den Router kontrolliert werden. Die Cisco IOS Software bietet eine Reihe von Optionen zur Beschränkung des Zugriffs auf die verschiedenen Schnittstellen. Dazu gehören die Network Foundation Protection (NFP)-Funktionsfamilie, verschiedene Zugriffskontrollmechanismen für Verwaltungsschnittstellen und die ZFW-Kernzone. Prüfen Sie andere Funktionen, wie z. B. VTY-Zugriffskontrolle, Schutz auf Verwaltungsebene und SNMP-Zugriffskontrolle, um zu ermitteln, welche Kombination von Routersteuerungsfunktionen am besten für Ihre jeweilige Anwendung geeignet ist.

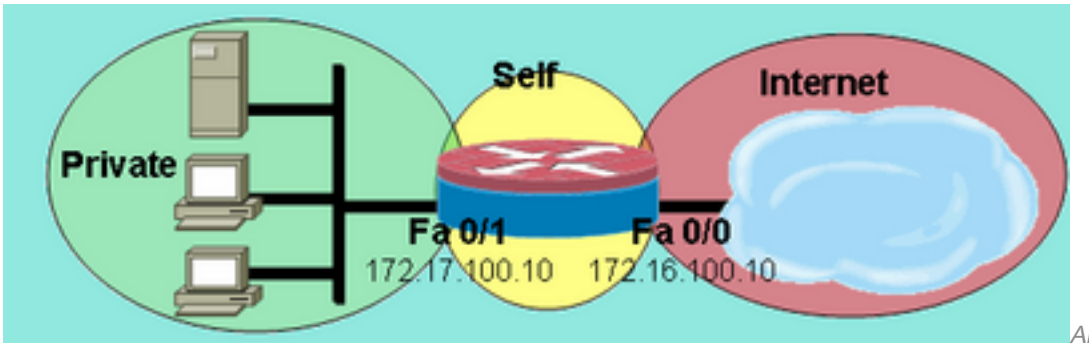
Im Allgemeinen eignet sich die NFP-Funktionsfamilie am besten für die Steuerung des Datenverkehrs, der für den Router selbst bestimmt ist. Informationen zum Schutz des Routers mit den NFP-Funktionen finden Sie unter Control Plane Security Overview in Cisco IOS Software.

Wenn Sie sich entscheiden, ZFW zur Steuerung des Datenverkehrs von und zu den IP-Adressen auf dem Router anzuwenden, müssen Sie berücksichtigen, dass die Firewall-Standardrichtlinien und -funktionen sich von denen unterscheiden, die für den Transitverkehr verfügbar sind. Transit-Datenverkehr ist definiert als Netzwerkverkehr, dessen Quell- und Ziel-IP-Adressen mit keiner der IP-Adressen übereinstimmen, die auf eine der Router-Schnittstellen angewendet werden, und der Datenverkehr bewirkt nicht, dass der Router beispielsweise Netzwerksteuerungsmeldungen wie ICMP-TTL-Ablauf oder nicht erreichbare Nachrichten für Netzwerk/Host sendet.

Die ZFW wendet eine standardmäßige Deny-All-Richtlinie auf Datenverkehr zwischen Zonen an, mit der Ausnahme, dass, wie in den allgemeinen Regeln erwähnt, Datenverkehr in jeder Zone, der direkt zu den Adressen der Router-Schnittstellen fließt, implizit zulässig ist. So wird sichergestellt, dass die Verbindung zu den Verwaltungsschnittstellen des Routers aufrechterhalten wird, wenn eine Zone-Firewall-Konfiguration auf den Router angewendet wird. Wenn die gleiche Deny-All-Richtlinie die direkte Verbindung zum Router betrifft, muss eine vollständige Konfiguration der Verwaltungsrichtlinie angewendet werden, bevor Zonen auf dem Router konfiguriert werden. Dies würde wahrscheinlich die Managementverbindung unterbrechen, wenn die Richtlinie nicht ordnungsgemäß implementiert oder in der falschen Reihenfolge angewendet würde.

Wenn eine Schnittstelle als Zonenelement konfiguriert ist, werden die mit der Schnittstelle verbundenen Hosts in die Zone eingeschlossen. Der Datenverkehr, der zu und von den IP-Adressen der Router-Schnittstellen fließt, wird jedoch nicht von den Zonenrichtlinien gesteuert (mit Ausnahme der in der Anmerkung in Abbildung 10 beschriebenen Fälle). Stattdessen werden bei der ZFW-Konfiguration automatisch alle IP-Schnittstellen des Routers in die Kernzone integriert. Um den IP-Datenverkehr zu steuern, der von den verschiedenen Zonen auf einem Router zu den Schnittstellen des Routers fließt, müssen Richtlinien angewendet werden, um Datenverkehr zwischen der Zone und der Kernzone des Routers zu blockieren oder zuzulassen/zu überprüfen und umgekehrt (siehe Abbildung 11).

Abbildung 11: Anwendung von Richtlinien zwischen Netzwerkzonen und Router-Kernzone



Anwendung von Richtlinien zwischen Netzwerkzonen und Router-Kernzone

Obwohl der Router eine Richtlinie für die Standardzugangsrichtlinie zwischen allen Zonen und der Kernzone bereitstellt, wird, wenn eine Richtlinie von einer Zone zur Kernzone konfiguriert wird und keine Richtlinie von der Kernzone zu den vom Benutzer konfigurierbaren, über die Schnittstelle verbundenen Zonen des Routers konfiguriert wird, der gesamte vom Router stammende Datenverkehr bei der Rückgabe an den Router auf die Richtlinie für die Verbindung von der Kernzone zur Kernzone trifft und blockiert. Daher muss der vom Router stammende Datenverkehr überprüft werden, um in die Kernzone zurückkehren zu können.

> **Anmerkung:** Die Cisco IOS Software verwendet stets die IP-Adresse, die mit den "nächstgelegenen" Ziel-Hosts einer Schnittstelle für den Datenverkehr wie Syslog, TFTP, Telnet und anderen Kontrollebenen-Services verknüpft ist, und unterwirft diesen Datenverkehr der Firewall-Richtlinie der Kernzone. Definiert ein Dienst jedoch eine bestimmte Schnittstelle als Quell-Schnittstelle mit Befehlen, die unter anderem die Quell-Schnittstelle [Typnummer] , die IP-TFTP-Quell-Schnittstelle [Typnummer] und die IP-Telnet-Quell-Schnittstelle [Typnummer] umfassen, wird der Datenverkehr der Kernzone unterworfen.

> **Hinweis:** Einige Dienste (insbesondere die Voice-over-IP-Dienste von Routern) verwenden ephemere oder nicht konfigurierbare Schnittstellen, die nicht Sicherheitszonen zugewiesen werden können. Diese Services funktionieren nicht ordnungsgemäß, wenn ihr Datenverkehr nicht mit einer konfigurierten Sicherheitszone verknüpft werden kann.

Richtlinien-Einschränkungen für die Self-Zone

Die Self-Zone-Richtlinie bietet im Vergleich zu den für die Transit-Datenverkehr-Zonenpaare verfügbaren Richtlinien nur einen begrenzten Funktionsumfang:

- Wie bei der klassischen Stateful-Inspection ist der vom Router generierte Datenverkehr auf TCP, UDP, ICMP und die Prüfung komplexer Protokolle für H.323 beschränkt.
- Anwendungsinspektion ist für Richtlinien in der Kernzone nicht verfügbar.
- Die Sitzungs- und Ratenbeschränkung kann nicht für Richtlinien der Kernzone konfiguriert werden.

Richtlinienkonfiguration für die Self-Zone

In den meisten Fällen sind dies wünschenswerte Zugriffsrichtlinien für Router-Managementservices:

- Verweigern Sie alle Telnet-Verbindungen, da das Klartext-Protokoll von Telnet leicht die

Anmeldeinformationen und andere vertrauliche Informationen preisgibt.
- Zulassen von SSH-Verbindungen von jedem Benutzer in jeder Zone SSH verschlüsselt Benutzeranmeldeinformationen und Sitzungsdaten und bietet so Schutz vor böswilligen Benutzern, die mithilfe von Paketerfassungstools Benutzeraktivitäten ausspionieren und Benutzeranmeldeinformationen oder vertrauliche Informationen wie die Routerkonfiguration gefährden. SSH Version 2 bietet besseren Schutz und behebt spezifische Schwachstellen, die in SSH Version 1 enthalten sind.
- Lassen Sie die HTTP-Verbindung zum Router aus den privaten Zonen zu, wenn die private Zone vertrauenswürdig ist. Wenn die private Zone andernfalls die Gefahr birgt, dass böswillige Benutzer Informationen kompromittieren, schützt HTTP den Managementverkehr nicht durch Verschlüsselung und gibt vertrauliche Informationen wie Benutzeranmeldeinformationen oder -konfigurationen preis.
- HTTPS-Verbindungen von jeder Zone zulassen. Ähnlich wie SSH verschlüsselt HTTPS Sitzungsdaten und Benutzeranmeldeinformationen.
- Beschränken Sie den SNMP-Zugriff auf einen bestimmten Host oder ein bestimmtes Subnetz. SNMP kann verwendet werden, um die Router-Konfiguration zu ändern und Konfigurationsinformationen anzuzeigen. SNMP muss mit Zugriffskontrolle für die verschiedenen Communitys konfiguriert werden.
- Blockieren von ICMP-Anfragen aus dem öffentlichen Internet an die Adresse der privaten Zone (dabei wird vorausgesetzt, dass die Adresse der privaten Zone routingfähig ist). Bei Bedarf können eine oder mehrere öffentliche Adressen für den ICMP-Verkehr zur Fehlerbehebung im Netzwerk verfügbar gemacht werden. Mehrere ICMP-Angriffe können dazu verwendet werden, Router-Ressourcen zu überlasten oder die Netzwerktopologie und -architektur zu überprüfen.

Ein Router kann diesen Richtlinientyp durch Hinzufügen von zwei Zonenpaaren für jede zu kontrollierende Zone anwenden. Jedes Zonenpaar für eingehenden oder ausgehenden Datenverkehr der Kernzone des Routers muss von der entsprechenden Richtlinie in die entgegengesetzte Richtung abgeglichen werden, es sei denn, der Datenverkehr geht nicht in die entgegengesetzte Richtung. Es kann jeweils eine Richtlinienzuweisung für eingehende und ausgehende Zonenpaare angewendet werden, die den gesamten Datenverkehr beschreibt, oder es können spezifische Richtlinienzuweisungen pro Zonenpaar angewendet werden. Die Konfiguration spezifischer Zonenpaare pro Richtlinienzuordnung ermöglicht die Anzeige von Aktivitäten, die den jeweiligen Richtlinienzuordnungen entsprechen.

In einem Beispielnetzwerk mit einer SNMP-Verwaltungsstation unter 172.17.100.11 und einem TFTP-Server unter 172.17.100.17 enthält diese Ausgabe ein Beispiel für die gesamte Zugriffsrichtlinie für die Verwaltungsschnittstelle:

```
class-map type inspect match-any self_service-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol h323
!
class-map type inspect match-all to-self-cmap
 match class-map self_service-cmap
 match access-group 120
!
class-map type inspect match-all from-self-cmap
 match class-map self_service-cmap
!
```

```
class-map type inspect match-all tftp-in-cmap
 match access-group 121
!
class-map type inspect match-all tftp-out-cmap
 match access-group 122
!
policy-map type inspect to-self-pmap
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
zone security private
zone security internet
zone-pair security priv-self source private destination self
 service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
 service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
 service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
 service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
 ip address 172.16.100.10
 zone-member security internet
!
interface FastEthernet 0/1
 ip address 172.17.100.10
 zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17
```

Leider bietet die Self-Zone-Richtlinie keine Möglichkeit, TFTP-Übertragungen zu überprüfen. Daher muss die Firewall den gesamten Datenverkehr zum und vom TFTP-Server weiterleiten, wenn TFTP die Firewall passieren muss.

Wenn der Router IPSec-VPN-Verbindungen beendet, müssen Sie auch eine Richtlinie für die Weiterleitung von IPSec ESP, IPSec AH, ISAKMP und NAT-T IPSec (UDP 4500) definieren. Dies hängt von den benötigten Services ab. Diese nächste Richtlinie kann zusätzlich zur oben angegebenen Richtlinie angewendet werden. Beachten Sie die Änderung der Richtlinienzuordnungen, bei denen eine Klassenzuordnung für den VPN-Datenverkehr mit einer Übergabeaktion eingefügt wurde. In der Regel ist verschlüsselter Datenverkehr vertrauenswürdig, es sei denn, Ihre Sicherheitsrichtlinie sieht vor, dass Sie verschlüsselten Datenverkehr von und zu angegebenen Endpunkten zulassen müssen.

```
class-map type inspect match-all crypto-cmap
 match access-group 123
!
policy-map type inspect to-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500
```

Zonenbasierte Firewall- und WAN-Services

Im Versionshinweis für Cisco Wide Area Application Services (Softwareversion 4.0.13) - Neue Funktionen für Softwareversion 4.0.13 finden Sie einen Anwendungshinweis mit Konfigurationsbeispielen und Anleitungen zur Verwendung.

Überwachung der zonenbasierten Firewall mit Befehlen zum Anzeigen und Debuggen

Die ZFW führt neue Befehle ein, um die Richtlinienkonfiguration anzuzeigen und die Firewall-Aktivität zu überwachen.

Zonenbeschreibung und Schnittstellen in einem angegebenen Bereich anzeigen:

```
show zone security [<zone-name>]
```

Wenn der Zonenname nicht enthalten ist, zeigt der Befehl die Informationen aller konfigurierten Zonen an.

```
Router#show zone security z1
zone z1
  Description: this is test zone1
  Member Interfaces:
    Ethernet0/0
```

Zeigt die Quellzone, Zielzone und die mit dem Zonenpaar verbundene Richtlinie an:

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

Wenn keine Quelle oder kein Ziel angegeben ist, werden alle Zonenpaare mit Quelle, Ziel und der

zugehörigen Richtlinie angezeigt. Wenn nur die Quell-/Zielzone angegeben wird, werden alle Zonenpaare angezeigt, die diese Zone als Quelle/Ziel enthalten.

```
Router#show zone-pair security
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

Zeigt eine angegebene Richtlinienzuordnung an:

```
show policy-map type inspect [<policy-map-name> [class <class-map-name]]
```

Wenn der Name einer Richtlinienzuordnung nicht angegeben ist, werden alle Richtlinienzuordnungen des Typs inspect (zusammen mit Layer-7-Richtlinienzuordnungen, die einen Untertyp enthalten) angezeigt.

```
Router#show policy-map type inspect p1
 Policy Map type inspect p1
   Class c1
    Inspect
```

Zeigt die Statistiken des Typs "policy-map" für die Laufzeitüberprüfung an, die sich derzeit auf einem angegebenen Zonenpaar befinden.

```
show policy-map type inspect zone-pair [zone-pair-name] [sessions]
```

Wenn kein Zonenpaarname erwähnt wird, werden Richtlinienzuordnungen für alle Zonenpaare angezeigt.

Die Sitzungsoption zeigt die Prüfsitzungen an, die von der Richtlinienzuordnungsanwendung für das angegebene Zonenpaar erstellt wurden.

```
Router#show policy-map type inspect zone-pair zp
 Zone-pair: zp

  Service-policy : p1

    Class-map: c1 (match-all)
      Match: protocol tcp
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: c2 (match-all)
      Match: protocol udp
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
```

```
      Drop
        0 packets, 0 bytes
```

Das urlfilter-Schlüsselwort zeigt die urlfilter-bezogenen Statistiken an, die sich auf die angegebene Richtlinienzuordnung beziehen (oder Richtlinienzuordnungen für alle Ziele, wenn kein Zonenpaarname angegeben ist):

```
show policy-map type inspect zone-pair [zone-pair-name] [urlfilter [cache]]
```

Wenn das Schlüsselwort cache zusammen mit urlfilter angegeben wird, wird der urlfilter-Cache (von IP-Adressen) angezeigt.

Zusammenfassung des Befehls show policy-map für inspect policy-maps:

```
show policy-map type inspect inspect { <policy name> [class <class name>] |
                  zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```

Zonenbasierter Firewall-Denial-of-Service-Schutz

Die ZFW bietet DoS-Schutz, um Netzwerktechniker über drastische Veränderungen der Netzwerkaktivität zu informieren und unerwünschte Aktivitäten zu minimieren, um die Auswirkungen von Änderungen der Netzwerkaktivität zu reduzieren. Die ZFW unterhält für jede Klassenzuordnung einen eigenen Zähler. Wenn also eine Klassenzuordnung für die Richtlinienzuordnungen zweier verschiedener Zonenpaare verwendet wird, werden zwei unterschiedliche DoS-Schutzindikatorensätze angewendet.

Die ZFW bietet standardmäßig vor Version 12.4(11)T eine Reduzierung von DoS-Angriffen auf Cisco IOS-Software. Das standardmäßige DoS-Schutzverhalten hat sich in Version 12.4(11)T der Cisco IOS-Software geändert.

Weitere Informationen zu TCP-SYN-DoS-Angriffen finden Sie unter Defining Strategies to Protect Against TCP SYN Denial of Service Attacks.

Anhänge

Anhang A: Basiskonfiguration

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 bridge-group 1
!
interface Vlan2
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
!
end
```

Anhang B: Endgültige (vollständige) Konfiguration

```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
```

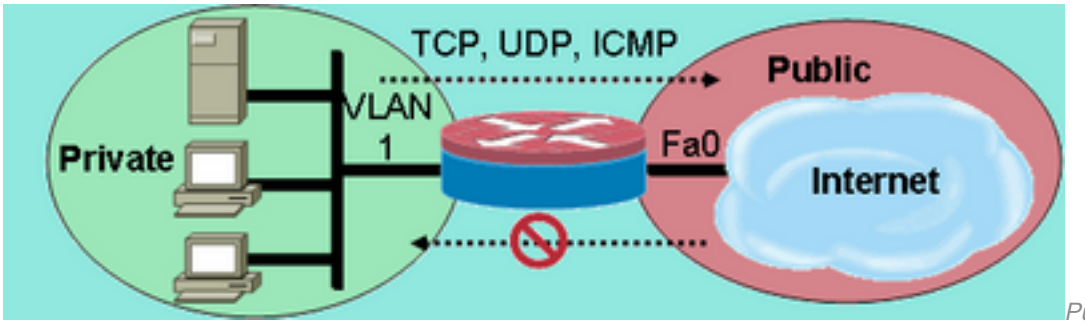
```
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match  port-misuse all
 match  strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
```

```
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
!
bridge 1 protocol ieee
bridge 1 route ip
!
End
```

Anhang C: Grundlegende Firewall-Konfiguration mit Zonenrichtlinien für zwei Zonen

Dieses Beispiel bietet eine einfache Konfiguration als Grundlage zum Testen von Funktionen für Erweiterungen der Cisco IOS Software ZFW. Bei dieser Konfiguration handelt es sich um eine Modellkonfiguration für zwei Zonen, die auf einem 1811-Router konfiguriert wurde. Die private Zone wird auf die festen Switch-Ports des Routers angewendet, sodass alle Hosts an den Switch-Ports mit VLAN 1 verbunden sind. Die öffentliche Zone wird auf FastEthernet 0 angewendet (siehe Abbildung 12).

Abbildung 12: Public Zone auf FastEthernet 0



Public Zone auf FastEthernet 0

```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
 class type inspect private-allowed-class
  inspect
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect private-allowed-policy
!
interface fastethernet 0
 zone-member security public
!
interface VLAN 1
 zone-member security private
```

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.